Red Hat Enterprise Virtualization 3.5 User Guide

Accessing and Using Virtual Machines from the User Portal

Red Hat Enterprise Virtualization Documentation Team

Red Hat Enterprise Virtualization 3.5 User Guide

Accessing and Using Virtual Machines from the User Portal

Red Hat Enterprise Virtualization Documentation Team
Red Hat Customer Content Services
rhev-docs@redhat.com

Legal Notice

Copyright © 2015 Red Hat.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This document shows you how to use virtual machines from the Red Hat Enterprise Virtualization User Portal.

Table of Contents

Part I. Getting Started 3

Chapter 1. Accessing the User Portal 4
1.1. Browser Requirements 4
1.2. Logging in to the User Portal 4
1.3. Logging out of the User Portal 6
1.4. Logging in for the First Time: Installing the Engine Certificate 6

Chapter 2. Installing Supporting Components 8
2.1. Installing Console Components 8
2.2. Installing USB Redirection Components 10

Part II. Basic Usage 12

Chapter 3. The Basic Tab 13
3.1. Basic Tab Graphical Interface 13
3.2. Running Virtual Machines 14

Chapter 4. The Extended Tab 19
4.1. The Extended Tab Graphical Interface 19
4.2. Running Virtual machines 21
4.3. Creating Virtual Machines 23
4.4. Explanation of Settings and Controls in the New Virtual Machine and Edit Virtual Machine Windows 27
4.5. Configuring Virtual Machines 40
4.6. Editing Virtual Machines 51
4.7. Removing Virtual Machines 56
4.8. Cloning Virtual Machines 56
4.9. Snapshots 57
4.10. Templates 61
4.11. Resources 74
4.12. Virtual Machines and Permissions 76

Part III. Advanced Usage 81
1. Introduction to Using Virtual Machines - Advanced 81

Chapter 5. Guest Drivers and Agents 82
5.1. Installing the Guest Agents and Drivers 82
5.2. Installing the Guest Agents and Drivers on Red Hat Enterprise Linux 82
5.3. Installing the Guest Agents and Drivers on Windows 82
5.4. Automating Guest Additions on Windows Guests with Red Hat Enterprise Virtualization Application Provisioning Tool(APT) 84
5.5. Red Hat Enterprise Virtualization Guest Drivers and Guest Agents 85

Chapter 6. Configuring Console Options 89
6.1. Console Options 89
6.2. Remote Viewer Options 94

Chapter 7. Configuring Multiple Monitors 98
7.1. Configuring Multiple Displays for Red Hat Enterprise Linux Virtual Machines 98
7.2. Changing the Resolution of Displays in a Red Hat Enterprise Linux Virtual Machine 98
7.3. Configuring Multiple Displays for Windows Virtual Machines 98
7.4. Changing the Resolution of Displays in a Windows Virtual Machine 99

Chapter 8. Configuring USB Devices 101

8.1. Using USB Devices on Virtual Machines - Introduction 101
8.2. Using USB Devices on Virtual Machines - Native Mode 101
8.3. Using USB Devices on a Windows Client 102
8.4. Using USB Devices on a Red Hat Enterprise Linux Client 102
8.5. Using USB Devices on Virtual Machines - Legacy Mode 103
8.6. Configuring a Linux Client to Use USB Redirection in Legacy Mode 106
8.7. Configuring a Windows Client to Use USB Redirection in Legacy Mode 107

Chapter 9. Configuring Single Sign-On for Virtual Machines 110
9.1. Configuring Single Sign-On for Virtual Machines 110
9.2. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines Using IPA (IdM) 110
9.3. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines Using Active Directory 111
9.4. Configuring Single Sign-On for Windows Virtual Machines 113
9.5. Disabling Single Sign-on for Virtual Machines 114

Revision History 115

Part I. Getting Started

Chapter 1. Accessing the User Portal

1.1. Browser Requirements

Use a supported web browser to access the Administration Portal and the User Portal. The portals support the following browsers:

- Red Hat Enterprise Linux 5.x - Mozilla Firefox 31
- Red Hat Enterprise Linux 6 - Mozilla Firefox 31
- Windows 7 - Internet Explorer 9 or later
- Windows Server 2008 - Internet Explorer 9 or later

1.2. Logging in to the User Portal

Log in to the Red Hat Enterprise Virtualization User Portal directly from your web browser.

Procedure 1.1. Logging in to the User Portal

1. Enter the provided **User Portal URL** in the address bar of your web browser. The address must be in the format of **`https://server.example.com/UserPortal`**. The login screen displays.

   Alternately, enter the provided **server address** into the web browser, to access the welcome screen. Click **`User Portal`** to be directed to the User Portal.

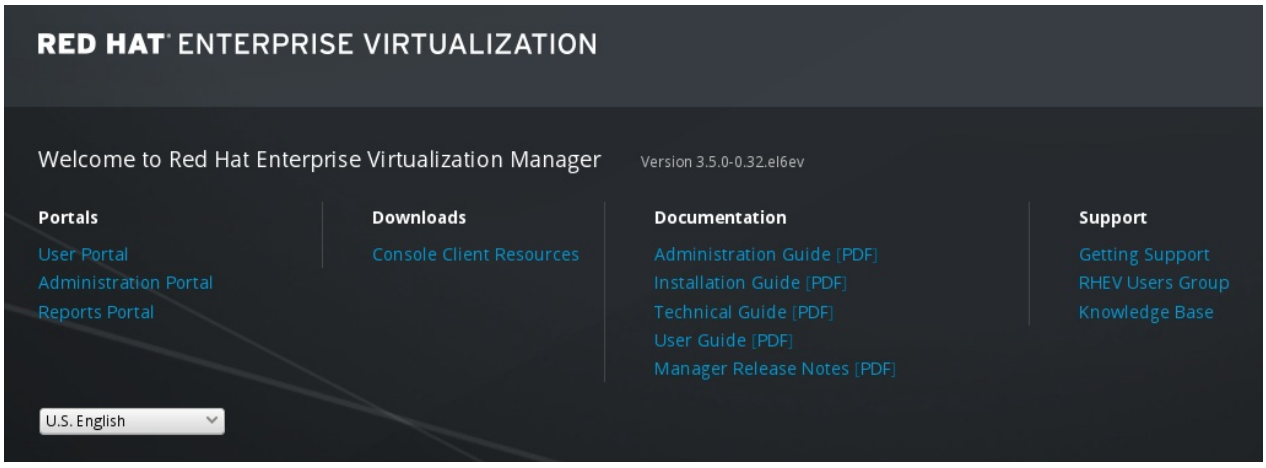


Figure 1.1. The User Portal Login Selection Screen

2. Enter your **User Name** and **Password**. Use the **Profile** drop-down menu to select the correct domain.

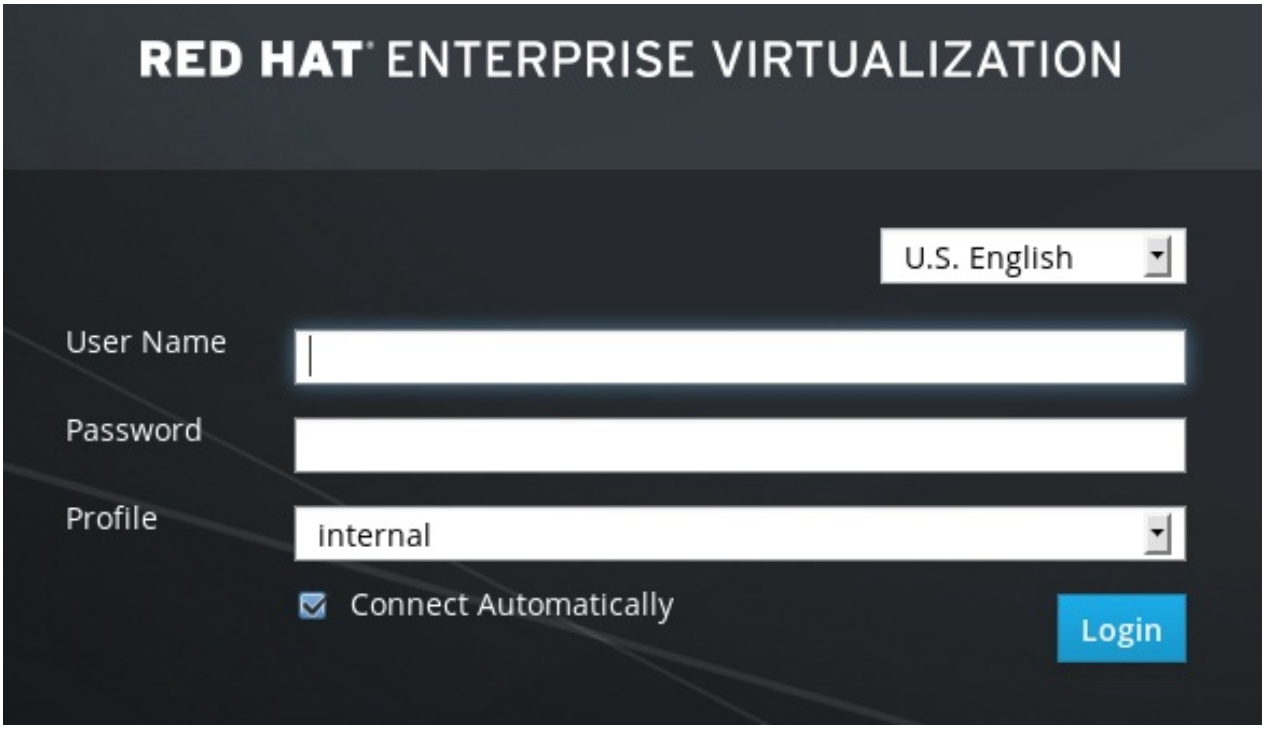


Figure 1.2. The User Portal Login Screen

- If you have only one running virtual machine in use, select the **Connect Automatically** check box and connect directly to your virtual machine.
- If you have more than one running virtual machine or do not want to automatically connect to a virtual machine, do not select the **Connect Automatically** check box.
- Select the language in which the User Portal is presented by using the drop-down menu at the lower-right of the login window.

3. Click **Login**. The list of virtual machines assigned to you displays.

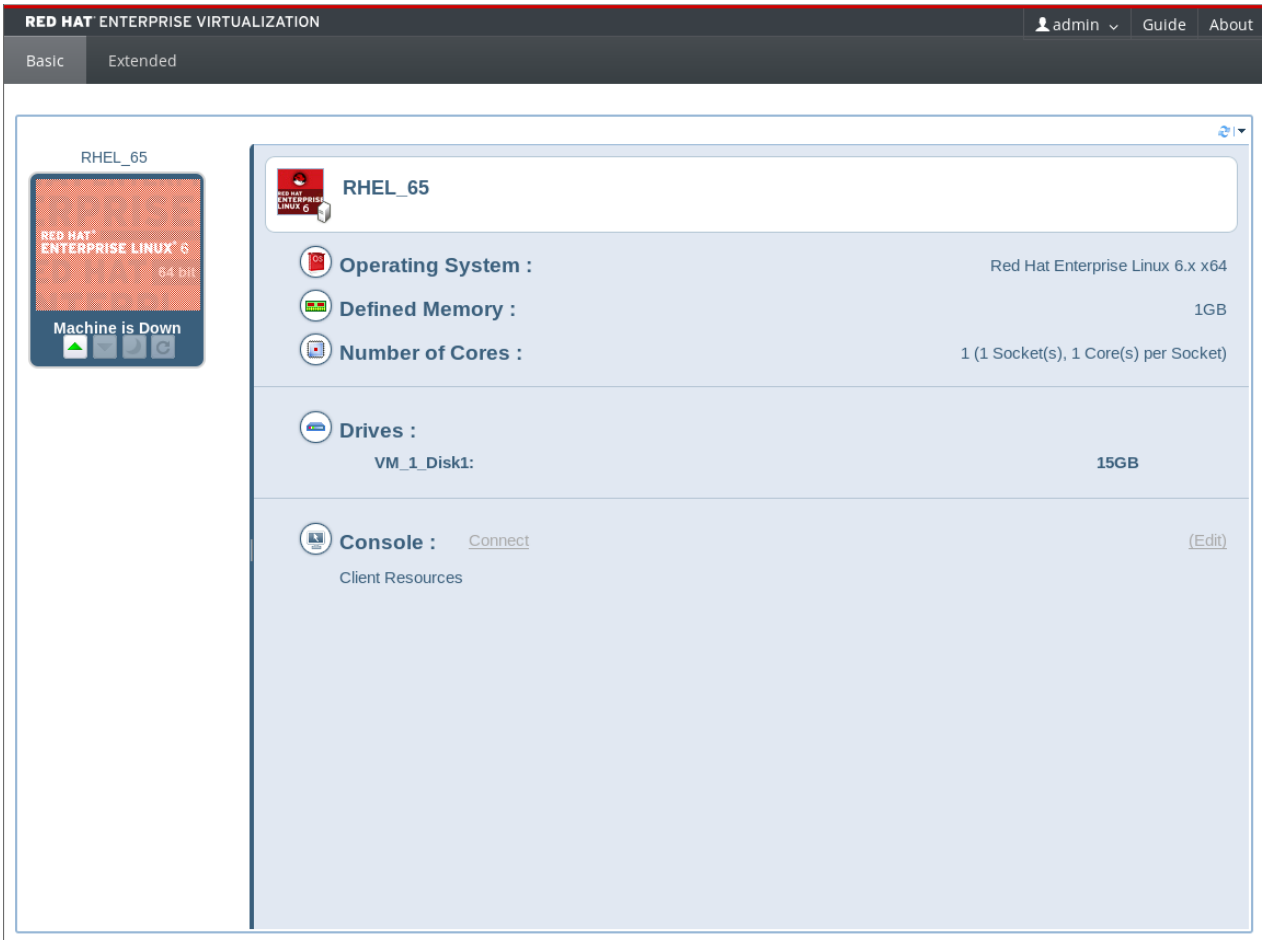


Figure 1.3. User Portal

1.3. Logging out of the User Portal

In the title bar of the User Portal, click your user name, then click **Sign out**. You are logged out and the User Portal login screen displays.

1.4. Logging in for the First Time: Installing the Engine Certificate

1.4.1. Installing the Red Hat Enterprise Virtualization Manager Certificate in Firefox

Summary

The first time you access the User Portal, you must install the certificate used by the Red Hat Enterprise Virtualization Manager to avoid security warnings.

Procedure 1.2. Installing the Red Hat Enterprise Virtualization Manager Certificate in Firefox

1. Navigate to the URL for the User Portal in Firefox.
2. Click **Add Exception** to open the **Add Security Exception** window.
3. Ensure the **Permanently store this exception** check box is selected.
4. Click the **Confirm Security Exception** button.

Result

You have installed the certificate used by the Red Hat Enterprise Virtualization Manager and security warnings no longer appear when you access the User Portal.

1.4.2. Installing the Red Hat Enterprise Virtualization Manager Certificate in Internet Explorer

Summary

The first time you access the User Portal, you must install the certificate used by the Red Hat Enterprise Virtualization Manager to avoid security warnings.

Procedure 1.3. Installing the Red Hat Enterprise Virtualization Manager Certificate in Internet Explorer

1. Navigate to the following URL:

   ```
   https://[your manager's address]/ca.crt
   ```

2. Click the **Open** button in the **File Download - Security Warning** window to open the **Certificate** window.
3. Click the **Install Certificate** button to open the **Certificate Import Wizard** window.
4. Select the **Place all certificates in the following store** radio button and click **Browse** to open the **Select Certificate Store** window.
5. Select **Trusted Root Certification Authorities** from the list of certificate stores, then click **OK**.
6. Click **Next** to proceed to the **Certificate Store** screen.
7. Click **Next** to proceed to the **Completing the Certificate Import Wizard** screen.
8. Click **Finish** to install the certificate.

Result

You have installed the certificate used by the Red Hat Enterprise Virtualization Manager and security warnings no longer appear when you access the User Portal.

Important

If you are using Internet Explorer to access the User Portal, you must also add the URL for the Red Hat Enterprise Virtualization welcome page to the list of trusted sites to ensure all security rules for trusted sites are applied to console resources such as **console.vv** mime files and Remote Desktop connection files.

Chapter 2. Installing Supporting Components

2.1. Installing Console Components

2.1.1. Console Components

A console is a graphical window that allows you to view the start up screen, shut down screen, and desktop of a virtual machine, and to interact with that virtual machine in a similar way to a physical machine. In Red Hat Enterprise Virtualization, the default application for opening a console to a virtual machine is Remote Viewer, which must be installed on the client machine prior to use.

2.1.2. Installing Remote Viewer on Linux

Remote Viewer is a SPICE client that is included the *virt-viewer* package provided by the **Red Hat Enterprise Linux Workstation (v. 6 for x86_64)** channel.

1. Install the *spice-xpi* package and dependencies:

```
# yum install spice-xpi
```

2. Check whether the **virt-viewer** package has already been installed on your system:

```
# rpm -q virt-viewer
virt-viewer-0.5.2-18.el6_4.2.x86_64
```

3. If the *virt-viewer* package has not been installed, install the package and its dependencies:

```
# yum install virt-viewer
```

4. Restart your browser for the changes to take effect.

The SPICE plug-in is installed. You can now connect to your virtual machines using the SPICE protocol.

2.1.3. Installing Remote Viewer for Internet Explorer on Windows

Summary

The SPICE ActiveX component is required to run Remote Viewer, which opens a graphical console to virtual machines. Remote Viewer is a SPICE client installed together with the SPICE ActiveX component; both are provided in the **SpiceX.cab** file.

Procedure 2.1. Installing Remote Viewer for Internet Explorer on Windows

1. Open Internet Explorer and log in to the User Portal.
2. Start a virtual machine and attempt to connect to the virtual machine using the **Browser plugin** console option.
3. Click the warning banner and click **Install This Add-on** when prompted.
4. Click **Install** when prompted.
5. Restart Internet Explorer for your changes to take effect.

Result

You have installed the SPICE plug-in and Remote Viewer, and can now connect to virtual machines using the SPICE protocol from within Internet Explorer.

2.1.4. Installing Remote Viewer on Windows

1. Open a web browser and download one of the following installers according to the architecture of your system.
   - Virt Viewer for 32-bit Windows:

     ```
     https://your-manager-fqdn/ovirt-engine/services/files/spice/virt-viewer-x86.msi
     ```

   - Virt Viewer for 64-bit Windows:

     ```
     https://your-manager-fqdn/ovirt-engine/services/files/spice/virt-viewer-x64.msi
     ```

2. Open the folder where the file was saved.
3. Double-click the file.
4. Click **Run** if prompted by a security warning.
5. Click **Yes** if prompted by User Account Control.

2.1.5. Manually Associating console.vv Files with Remote Viewer

Summary

If you are prompted to download a **console.vv** file when attempting to open a console to a virtual machine using the native client console option, and Remote Viewer is already installed, then you can manually associate **console.vv** files with Remote Viewer so that Remote Viewer can automatically use those files to open consoles.

Procedure 2.2. Manually Associating console.vv Files with Remote Viewer

1. A. In the User Portal **Basic** tab, select the virtual machine and click the **Edit** button of the **Console** section of the display pane to open the **Console Options** window.

Figure 2.1. Opening the Console Options window in the Basic tab

B. In the User Portal **Extended** tab, click the **Edit Console Options** button of a virtual machine to open the **Console Options** window.

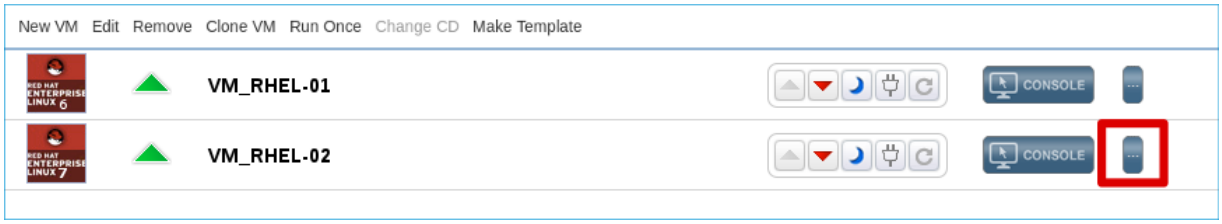


Figure 2.2. Opening the Console Options window in the Extended tab

2. Change the console invocation method to **Native client** and click **OK**.
3. Start the virtual machine.
4. Attempt to open a console to the virtual machine, then click **Save** when prompted to open or save the **console.vv** file.
5. Use Windows Explorer to navigate to the location on your local machine where you saved the file.
6. Double-click the **console.vv** file and select **Select a program from a list of installed programs** when prompted.
7. In the **Open with** window, select **Always use the selected program to open this kind of file** and click the **Browse** button.
8. Navigate to the **C:\Users*[user name]*\AppData\Local\virt-viewer\bin** directory and select **remote-viewer.exe**.
9. Click **Open** and then click **OK**.

Result

You have manually associated the **console.vv** file with Remote Viewer. When you use the native client console invocation option to open a console to a virtual machine, Remote Viewer will automatically use the **console.vv** file that the Red Hat Enterprise Virtualization Manager provides to open a console to that virtual machine without prompting you to select the application to use.

2.2. Installing USB Redirection Components

2.2.1. Installing USB Clerk on Windows

USB Clerk provides a service that is able to install and uninstall Windows USB drivers in guest virtual machines.

Procedure 2.3. Installing USB Clerk on Windows

1. Open a web browser and download one of the following installers according to the architecture of your system.
   - USB Clerk for 32-bit Windows:

```
https://[your manager's address]/ovirt-
engine/services/files/spice/usbclerk-x86.msi
```

- USB Clerk for 64-bit Windows:

```
https://[your manager's address]/ovirt-
engine/services/files/spice/usbclerk-x64.msi
```

2. Open the folder where the file was saved.
3. Double-click the file.
4. Click **Run** if prompted by a security warning.
5. Click **Yes** if prompted by User Account Control.

Result

USB Clerk is installed. The SPICE client sends requests to install or uninstall drivers for USB devices when users connect or disconnect USB devices to or from a guest, upon request.

Part II. Basic Usage

Chapter 3. The Basic Tab

3.1. Basic Tab Graphical Interface

The **Basic** tab enables you to view and use all the virtual machines that are available to you. The screen consists of three areas: the title bar, a virtual machines area, and a details pane. A number of control buttons allow you to work with the virtual machines.

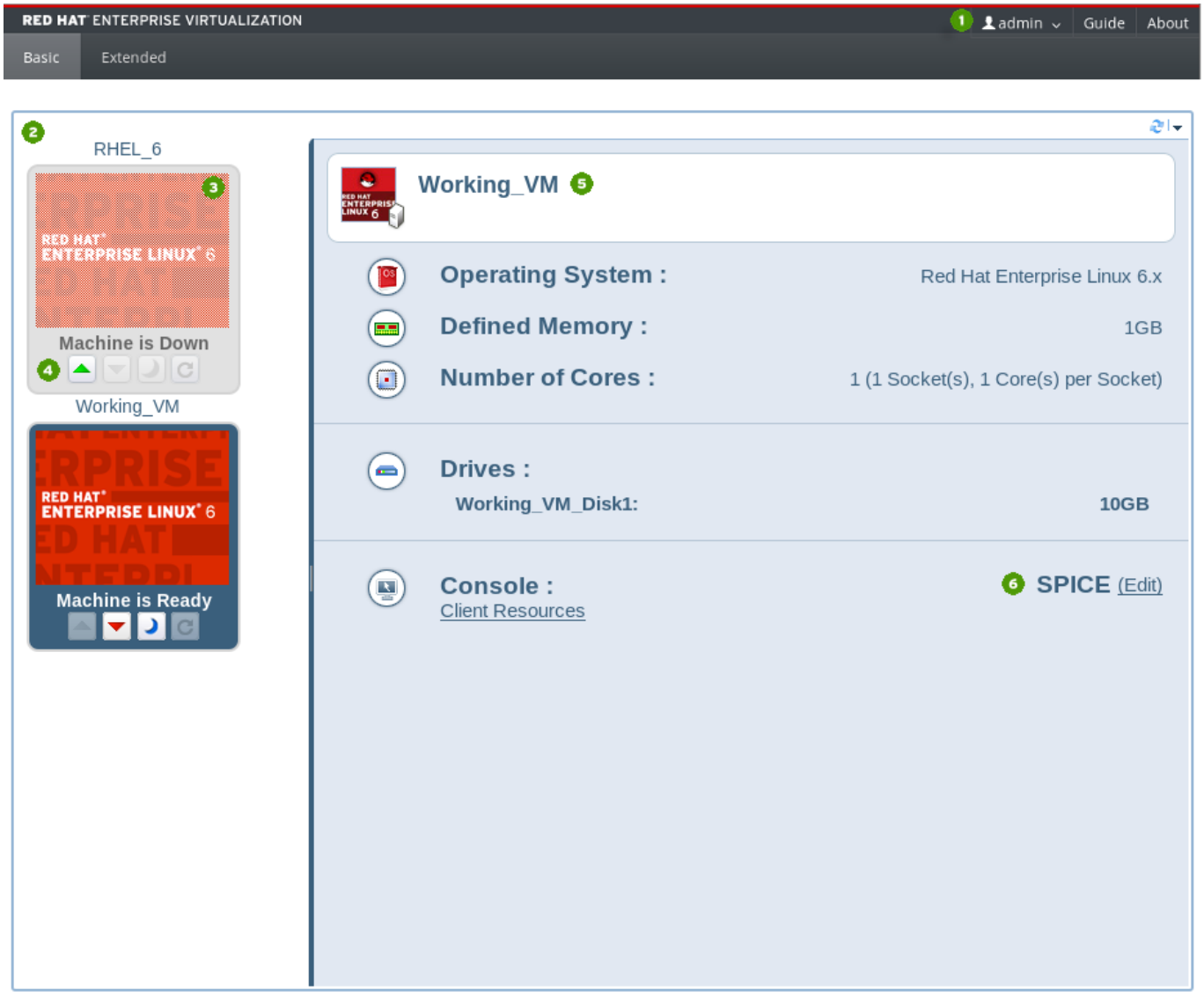


Figure 3.1. The User Portal

The title bar (1) includes the name of the **User** logged in to the portal and links to the **Guide** and **About** pages.

In the virtual machines area, the name of the virtual machines or virtual machine pools assigned to you display (2). The logo of the virtual machine's operating system also displays (3). When a virtual machine is powered up, you can connect to it by double-clicking on the virtual machine's logo.

On each virtual machine's icon, buttons allow you to play, stop or pause a virtual machine. The buttons perform the same functions as buttons on a media player (4).

- The green play button starts up the virtual machine. It is available when the virtual machine is paused, stopped or powered off.
- The red stop button stops the virtual machine. It is available when the virtual machine is running.
- The blue pause button temporarily halts the virtual machine. To restart it, press the green play button.
- The green reboot button reboots the virtual machine. It is available when the virtual machine is running.

The status of the virtual machine is indicated by the text below the virtual machine's icon - **`Machine is Ready`** or **`Machine is Down`**.

Clicking on a virtual machine displays the statistics of the selected virtual machine on the details pane to the right (5), including the operating system, defined memory, number of cores and size of virtual drives. You can also configure connection protocol options (6) such as enabling the use of USB devices or local drives.

3.2. Running Virtual Machines

3.2.1. Running Virtual Machines - Overview

In the User Portal, virtual machines are represented by icons that indicate both type and status. The icons indicate whether a virtual machine is part of a virtual machine pool or is a standalone Windows or Linux virtual machine. The icons also reflect whether the virtual machine is running or stopped.

The User Portal displays a list of the virtual machines assigned to you. You can turn on one or more virtual machines, connect, and log in. You can access virtual machines that are running different operating systems, and you can use multiple virtual machines simultaneously.

In contrast, if you have only one running virtual machine and have enabled automatic connection, you can bypass the User Portal and log in directly to the virtual machine, similar to how you log in to a physical machine.

3.2.2. Turning on a Virtual Machine

To use a virtual machine in the User Portal, you must turn it on and then connect to it. If a virtual machine is turned off, it is grayed out and displays **`Machine is Down`**.

You can be assigned an individual virtual machine or assigned to one or more virtual machines that are part of a virtual machine pool. Virtual machines in a pool are all clones of a base template, and have the same operating system and installed applications.

Note

When you take a virtual machine from a virtual machine pool, you are not guaranteed to receive the same VM each time. However, if you configure console options for a VM taken from a virtual machine pool, those options are saved as the default for all VMs taken from that virtual machine pool.

Procedure 3.1. Turning on a Virtual Machine

1. Turn on the standalone virtual machine or take a virtual machine from a pool as follows:

   - To turn on a standalone virtual machine, select the virtual machine icon and click the button.

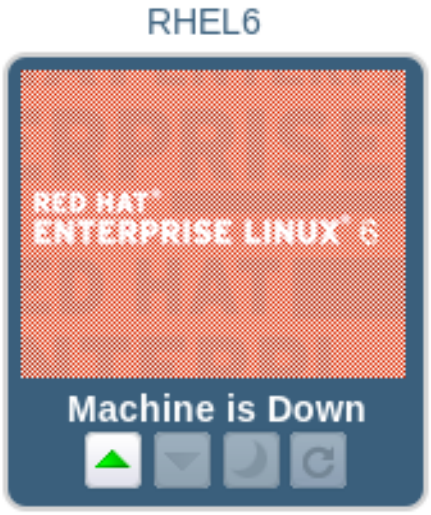


Figure 3.2. Turn on virtual machine

   - To take a virtual machine from a pool, select the virtual machine pool icon and click the button.

Figure 3.3. Take virtual machine from a pool

If there is an available virtual machine in the pool, an icon for that virtual machine will appear in your list. The rest of this procedure then applies to that virtual machine. If you can take multiple virtual machines from a pool, the icon for the virtual machine pool will change into an icon for the last virtual machine you have taken when you take the maximum number of virtual machines possible for that pool.

2. The virtual machine powers up.

Figure 3.4. Virtual machine powering up

3. When the virtual machine is powered up, the icon is no longer grayed out. The text displays as **`Machine is Ready`**. You are now ready to connect.

Figure 3.5. Virtual machine turned on

Note

You can only connect to a virtual machine after it has powered up.

3.2.3. Connecting to a Powered-On Virtual Machine

After a virtual machine has been turned on, you can connect to it, log in, and start work the same way that you would with a physical machine. The text "Machine is Ready" displays on virtual machines that are powered up.

Procedure 3.2. Connecting to a Powered on Virtual Machine

1. Double-click on the selected virtual machine to connect.

Figure 3.6. Connect to Virtual Machine

2. A console window of the virtual machine displays. You can now use the virtual machine in the same way that you would use a physical desktop.

Note

The first time you connect with SPICE, you are prompted to install the appropriate SPICE component or plug-in. If it is the first time you are connecting from a Red Hat Enterprise Linux computer, install the SPICE plug-in for Mozilla Firefox. If you are connecting from a Windows computer, install the ActiveX plug-in.

3.2.4. Logging out of a Virtual Machine

It is recommended that you log out from a virtual machine before shutting it down, to minimize the risk of data loss. Additionally, if you attempt to forcefully shut down a virtual machine from the User Portal, it might freeze with a status of **`Powering Down`**. To gracefully turn off a virtual machine, use the following steps.

Procedure 3.3. Shutting down a virtual machine

1. Log out of the guest operating system.
2. If you were using your virtual machine in full screen mode, press **`Shift`**+**`F11`** to exit full screen mode, and close the virtual machine's console window. You are now returned to the User Portal.
3. To shut down the virtual machine, click the button. The virtual machine is grayed out and displays as "Machine is Down" when it has been turned off.

Chapter 4. The Extended Tab

4.1. The Extended Tab Graphical Interface

The **Extended** tab graphical interface enables you to access and monitor all the virtual resources that are available to you. Eight elements of the **Extended** tab are explained below.

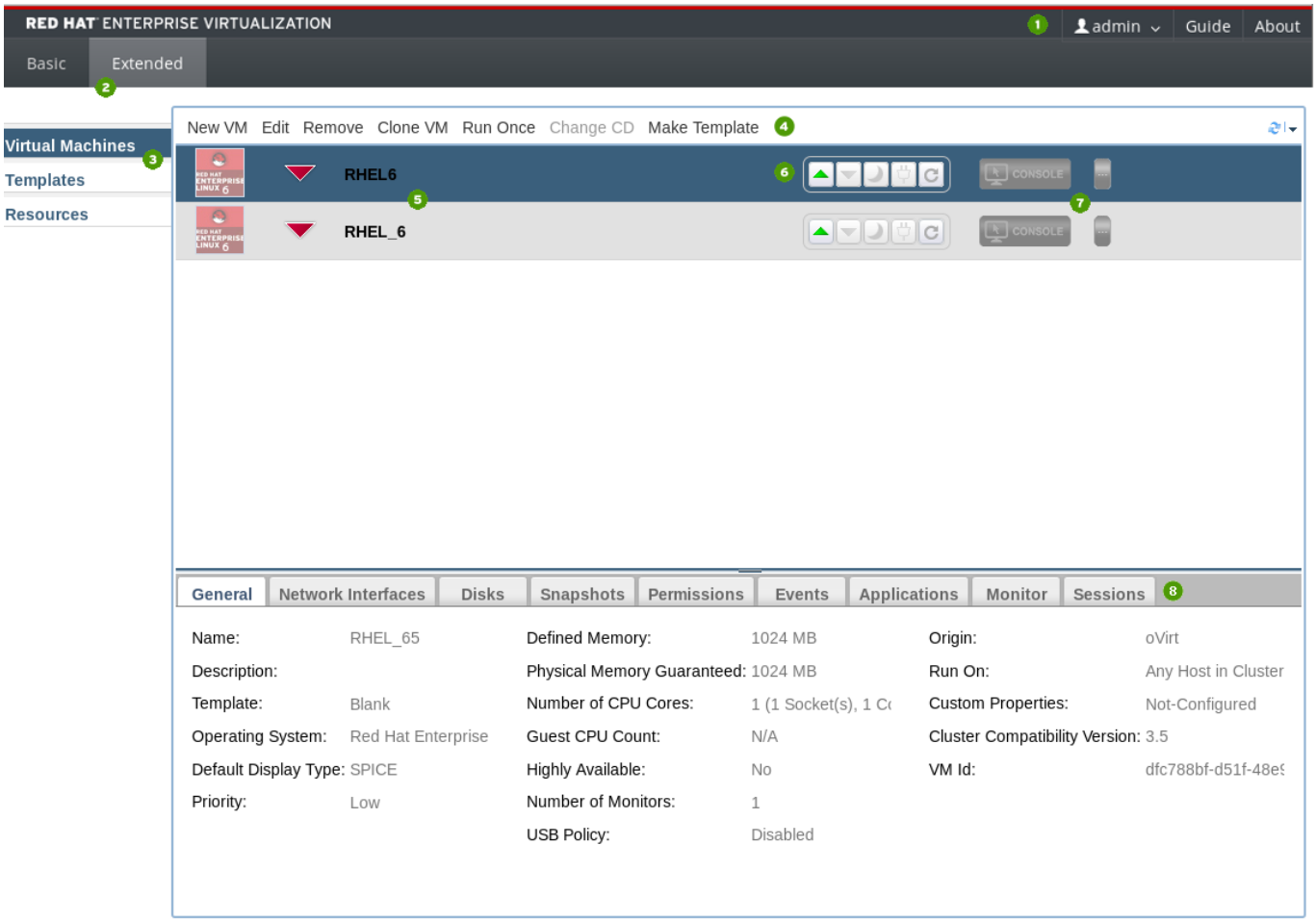


Figure 4.1. The Extended Tab

Table 4.1. The Extended Tab

Number	Element Name	Description
1	Title Bar	Includes the name of the **User** logged in to the portal and links to the **Guide** and **About** pages.
2	User Portal View Option Tabs	Power Users have access to the **Extended** tab of the User Portal and the **Basic** tab of the User Portal. The **Basic** view is the default view for users with basic permissions.

Number	Element Name	Description
3	Navigation Pane	The Navigation Pane allows you to toggle between the Virtual Machines, Templates, and Resources tabs.
4	Management Bar	The management bar is used to create and make changes to virtual machines.
5	Virtual Machine List	The list of virtual machines, with the operating systems installed on them and their statuses (running, paused, or stopped).
6	Virtual Machine Control Buttons	Virtual Machine Control Buttons allow you to play, stop, pause, or power off virtual machines. The green play button starts the virtual machine. It is available when the virtual machine is paused, stopped or powered off. The red stop button stops the virtual machine. It is available when the virtual machine is running. The blue pause button temporarily halts the virtual machine. To restart it, press the green play button. The power button turns off the virtual machine. It is available when the virtual machine is running. The reboot button restarts the virtual machine. It is available when the virtual machine is running.
7	Console Button	The console button launches a SPICE window and connects to machines that have been powered-up.
8	Details Pane	The Details Pane displays the statistics of the virtual machine selected in the Navigation Pane.

Details Pane Tab Functions:

- The **General** tab displays basic software and hardware information of the virtual machine, including its name, operating system, display protocol and defined memory.
- The **Network Interfaces** tab displays the name, type and speed of the network connected to the virtual machine. You can add, edit and remove network interfaces using this tab.
- The **Disks** tab displays the name, size and format of the disk attached to the virtual machine. You can add, edit and remove virtual disks using this tab.
- The **Snapshots** tab displays a view of the virtual machine's operating system and applications. You can create and use snapshots using this tab.
- The **Permissions** tab displays the users and roles assigned to each virtual machine. You can assign and remove user permissions using this tab.
- The **Events** tab displays the description and time of events which affect the virtual machine.
- The **Applications** tab displays the applications which have been installed on the virtual machine.
- The **Monitor** tab displays the CPU Usage, Memory Usage, and Network Usage statistics for the machine selected in the Navigation Pane.
- The **Sessions** tab displays the Logged-In User, Console User, and Console Client IP for the machine selected in the Navigation Pane.

4.2. Running Virtual machines

4.2.1. Connecting to Virtual Machines

After you have logged into the portal, you can start, stop, or connect to the virtual machines that are displayed.

Summary

This procedure describes how to start a stopped virtual machine, and how to connect to the virtual machine.

Procedure 4.1. Connecting to Virtual Machines

1.

Figure 4.2. Virtual machine turned off

Select the virtual machine to which you want to connect, then click the Play button. The virtual machine powers up. The Stop symbol next to the virtual machine's name changes to a Powering Up symbol.

When the virtual machine is turned on, the Play symbol displays next to the virtual machine's name.

Figure 4.3. Virtual machine turned on

2. Click the **Console** button to connect to the virtual machine.

Figure 4.4. Connect to virtual machine

3. If it is the first time connecting with SPICE, you will be prompted to install the appropriate SPICE component or plug-in. If you are connecting from a Windows computer, install the ActiveX component. If you are connecting from a Red Hat Enterprise Linux computer, install the Mozilla Firefox plug-in.

A console window of the virtual machine displays. You can now use the virtual machine in the same way that you would use a physical desktop.

Result

You have started a stopped virtual machine and connected to it.

Warning

By default, a virtual machine running Windows 7 will be suspended after an hour of inactivity. This prevents users from connecting to the virtual machine from the User Portal. To avoid this, disable the power-saving feature on the guest's power manager.

4.2.2. Turning Off a Virtual Machine from the User Portal

If you attempt to turn off a virtual machine from the User Portal, it might freeze with a status of **Powering Down**, indicating that it has not completely shut down. Use the following procedure to gracefully turn off a virtual machine from within the User Portal.

Important

To minimize the risk of data loss, log off from a virtual machine before turning it off.

Summary

This procedure explains how to turn off a virtual machine from the User Portal.

Procedure 4.2. Turning Off a Virtual Machine from the User Portal

1. Log out of the guest operating system.
2. If you were using your virtual machine in full screen mode, press **Shift**+**F11** to exit full screen mode, and close the virtual machine's console window. You are now returned to the User Portal.
3. To turn off the virtual machine, click the button. The Stop symbol appears next to the

name of the virtual machine when it has been turned off.

Result

You have turned off a virtual machine.

Note

You can also turn off virtual machines gracefully using the native method from within the virtual machine itself. For example, in Windows virtual machines you can click **Start → Shut Down**, and in Red Hat Enterprise Linux virtual machines you can click **System → Shut Down**.

4.2.3. Rebooting a Virtual Machine from the User Portal

Important

To minimize the risk of data loss, log off from a virtual machine before rebooting.

Summary

This procedure explains how to reboot a virtual machine from the User Portal.

Procedure 4.3. Rebooting a Virtual Machine from the User Portal

1. Log out of the guest operating system.
2. If you were using your virtual machine in full screen mode, press **Shift+F11** to exit full screen mode, and close the virtual machine's console window. You are now returned to the User Portal.
3. To reboot the virtual machine, click the button. The Reboot symbol appears next to the name of the virtual machine while it is rebooting, then changes back to a Play symbol when reboot completes.

Result

You have rebooted a virtual machine.

4.3. Creating Virtual Machines

4.3.1. Creating a Virtual Machine

Summary

You can create a virtual machine using a blank template and configure all of its settings.

Procedure 4.4. Creating a Virtual Machine

1. Click the **Virtual Machines** tab.

2. Click the **New VM** button to open the **New Virtual Machine** window.

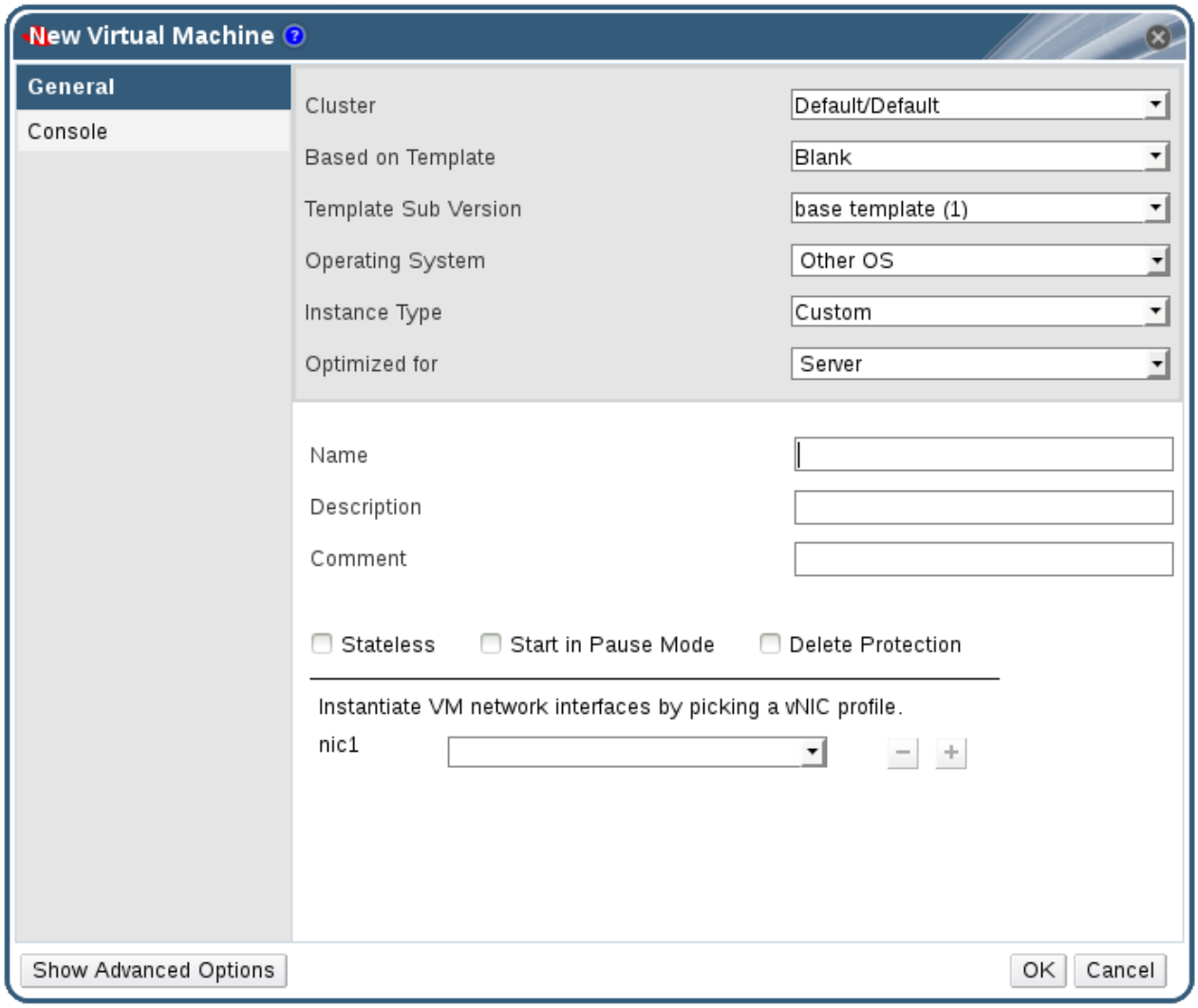


Figure 4.5. The New Virtual Machine Window

3. On the **General** tab, fill in the **Name** and **Operating System** fields. You can accept the default settings for other fields, or change them if required.

4. Alternatively, click the **Initial Run**, **Console**, **Host**, **Resource Allocation**, **Boot Options**, **Random Generator**, and **Custom Properties** tabs in turn to define options for your virtual machine.

5. Click **OK** to create the virtual machine and close the window.

   The **New Virtual Machine - Guide Me** window opens.

6. Use the Guide Me buttons to complete configuration or click **Configure Later** to close the window.

Result

The new virtual machine is created and displays in the list of virtual machines with a status of **Down**. Before you can use this virtual machine, add at least one network interface and one virtual disk, and install an operating system.

4.3.2. Creating a Virtual Machine Based on a Template

Create virtual machines based on templates. This allows you to create virtual machines that are pre-configured with an operating system, network interfaces, applications and other resources.

Note

Virtual machines created based on a template depend on that template. This means that you cannot remove that template from the Manager if there is a virtual machine that was created based on that template. However, you can clone a virtual machine from a template to remove the dependency on that template.

1. Click the **Virtual Machines** tab.
2. Click the **New VM** button to open the **New Virtual Machine** window.
3. Select the **Cluster** on which the virtual machine will run.
4. Select a template from the **Based on Template** list.
5. Select a template sub version from the **Template Sub Version** list.
6. Enter a **Name**, **Description**, and any **Comments**, and accept the default values inherited from the template in the rest of the fields. You can change them if needed.
7. Click the **Resource Allocation** tab.
8. Select the **Thin** radio button in the **Storage Allocation** area.
9. Select the disk provisioning policy from the **Allocation Policy** list. This policy affects the speed of the clone operation and the amount of disk space the new virtual machine initially requires.
   - Selecting **Thin Provision** results in a faster clone operation and provides optimized usage of storage capacity. Disk space is allocated only as it is required. This is the default selection.
   - Selecting **Preallocated** results in a slower clone operation and provides optimized virtual machine read and write operations. All disk space requested in the template is allocated at the time of the clone operation.
10. Use the **Target** list to select the storage domain on which the virtual machine's virtual disk will be stored.
11. Click **OK**.

The virtual machine is displayed in the list in the **Virtual Machines** tab.

4.3.3. Creating a Cloned Virtual Machine Based on a Template

Summary

Cloned virtual machines are similar to virtual machines based on templates. However, while a cloned virtual machine inherits settings in the same way as a virtual machine based on a template, a cloned virtual machine does not depend on the template on which it was based after it has been created.

Note

If you clone a virtual machine from a template, the name of the template on which that virtual machine was based is displayed in the **General** tab of the **Edit Virtual Machine** window for that virtual machine. If you change the name of that template, the name of the template in the **General** tab will also be updated. However, if you delete the template from the Manager, the original name of that template will be displayed instead.

Procedure 4.5. Cloning a Virtual Machine Based on a Template

1. Click the **Virtual Machines** tab.
2. Click the **New VM** button to open the **New Virtual Machine** window.
3. Select the **Cluster** on which the virtual machine will run.
4. Select a template from the **Based on Template** drop-down menu.
5. Select a template sub version from the **Template Sub Version** drop-down menu.
6. Enter a **Name**, **Description** and any **Comments**. You can accept the default values inherited from the template in the rest of the fields, or change them if required.
7. Click the **Resource Allocation** tab.
8. Select the **Clone** radio button in the **Storage Allocation** area.
9. Select the disk provisioning policy from the **Allocation Policy** drop-down menu. This policy affects the speed of the clone operation and the amount of disk space the new virtual machine initially requires.
   - Selecting **Thin Provision** results in a faster clone operation and provides optimized usage of storage capacity. Disk space is allocated only as it is required. This is the default selection.
   - Selecting **Preallocated** results in a slower clone operation and provides optimized virtual machine read and write operations. All disk space requested in the template is allocated at the time of the clone operation.
10. Use the **Target** drop-down menu to select the storage domain on which the virtual machine's virtual disk will be stored.
11. Click **OK**.

Note

Cloning a virtual machine may take some time. A new copy of the template's disk must be created. During this time, the virtual machine's status is first **Image Locked**, then **Down**.

Result

The virtual machine is created and displayed in the list in the **Virtual Machines** tab. You can now assign users to it, and can begin using it when the clone operation is complete.

4.4. Explanation of Settings and Controls in the New Virtual Machine and Edit Virtual Machine Windows

4.4.1. Virtual Machine General Settings Explained

The following table details the options available on the **General** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.2. Virtual Machine: General Settings

Field Name	Description
Cluster	The name of the host cluster to which the virtual machine is attached. Virtual machines are hosted on any physical machine in that cluster in accordance with policy rules.
Based on Template	The template on which the virtual machine can be based. This field is set to **Blank** by default, which allows you to create a virtual machine on which an operating system has not yet been installed.
Template Sub Version	The version of the template on which the virtual machine can be based. This field is set to the most recent version for the given template by default. If no versions other than the base template are available, this field is set to **base template** by default. Each version is marked by a number in brackets that indicates the relative order of the versions, with higher numbers indicating more recent versions.
Operating System	The operating system. Valid values include a range of Red Hat Enterprise Linux and Windows variants.
Instance Type	The instance type on which the virtual machine's hardware configuration can be based. This field is set to **Custom** by default, which means the virtual machine is not connected to an instance type. The other options available from this drop down menu are **Large**, **Medium**, **Small**, **Tiny**, **XLarge**, and any custom instance types that the Administrator has created. Other settings that have a chain link icon next to them are pre-filled by the selected instance type. If one of these values is changed, the virtual machine will be detached from the instance type and the chain icon will appear broken. However, if the changed setting is restored to its original value, the virtual machine will be reattached to the instance type and the links in the chain icon will rejoin.

Field Name	Description
Optimized for	The type of system for which the virtual machine is to be optimized. There are two options: **Server**, and **Desktop**; by default, the field is set to **Server**. Virtual machines optimized to act as servers have no sound card, use a cloned disk image, and are not stateless. In contrast, virtual machines optimized to act as desktop machines do have a sound card, use an image (thin allocation), and are stateless.
Name	The name of the virtual machine. Names must not contain any spaces, and must contain at least one character from A-Z or 0-9. The maximum length of a virtual machine name is 255 characters.
Description	A meaningful description of the new virtual machine.
Comment	A field for adding plain text human-readable comments regarding the virtual machine.
Stateless	Select this check box to run the virtual machine in stateless mode. This mode is used primarily for desktop VMs. Running a stateless desktop or server creates a new COW layer on the VM hard disk image where new and changed data is stored. Shutting down the stateless VM deletes the new COW layer, which returns the VM to its original state. Stateless VMs are useful when creating machines that need to be used for a short time, or by temporary staff.
Start in Pause Mode	Select this check box to always start the virtual machine in pause mode. This option is suitable for VMs which require a long time to establish a SPICE connection; for example, VMs in remote locations.
Delete Protection	Select this check box to make it impossible to delete the virtual machine. It is only possible to delete the virtual machine if this check box is not selected.

At the bottom of the **General** tab is a drop-down box that allows you to assign network interfaces to the new virtual machine. Use the plus and minus buttons to add or remove additional network interfaces.

4.4.2. Virtual Machine System Settings Explained

The following table details the options available on the **System** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.3. Virtual Machine: System Settings

Field Name	Description

Field Name	Description
Memory Size	The amount of memory assigned to the virtual machine. When allocating memory, consider the processing and storage needs of the applications that are intended to run on the virtual machine. Maximum guest memory is constrained by the selected guest architecture and the cluster compatibility level.
Total Virtual CPUs	The processing power allocated to the virtual machine as CPU Cores. Do not assign more cores to a virtual machine than are present on the physical host.
Cores per Virtual Socket	The number of cores assigned to each virtual socket.
Virtual Sockets	The number of CPU sockets for the virtual machine. Do not assign more sockets to a virtual machine than are present on the physical host.
Time Zone	This option sets the time zone offset of the guest hardware clock. For Windows, this should correspond to the time zone set in the guest. Most default Linux installations expect the hardware clock to be GMT+00:00.
Provide custom serial number policy	This checkbox allows you to specify a serial number for the virtual machine. Select either: - **Host ID**: Sets the host's UUID as the virtual machine's serial number. - **Vm ID**: Sets the virtual machine's UUID as its serial number. - **Custom serial number**: Allows you to specify a custom serial number.

4.4.3. Virtual Machine Initial Run Settings Explained

The following table details the options available on the **Initial Run** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows. The settings in this table are only visible if the **Use Cloud-Init/Sysprep** check box is selected, and certain options are only visible when either a Linux-based or Windows-based option has been selected in the **Operating System** list in the **General** tab, as outlined below.

Table 4.4. Virtual Machine: Initial Run Settings

Field Name	Operating System	Description
Use Cloud-Init/Sysprep	Linux, Windows	This check box toggles whether Cloud-Init or Sysprep will be used to initialize the virtual machine.
VM Hostname	Linux, Windows	The host name of the virtual machine.

Field Name	Operating System	Description
Domain	Windows	The Active Directory domain to which the virtual machine belongs.
Organization Name	Windows	The name of the organization to which the virtual machine belongs. This option corresponds to the text field for setting the organization name displayed when a machine running Windows is started for the first time.
Active Directory OU	Windows	The organizational unit in the Active Directory domain to which the virtual machine belongs.
Configure Time Zone	Linux, Windows	The time zone for the virtual machine. Select this check box and select a time zone from the **Time Zone** list.
Admin Password	Windows	The administrative user password for the virtual machine. Click the disclosure arrow to display the settings for this option. - **Use already configured password**: This check box is automatically selected after you specify an initial administrative user password. You must clear this check box to enable the **Admin Password** and **Verify Admin Password** fields and specify a new password. - **Admin Password**: The administrative user password for the virtual machine. Enter the password in this text field and the **Verify Admin Password** text field to verify the password.
Authentication	Linux	The authentication details for the virtual machine. Click the disclosure arrow to display the settings for this option. - **Use already configured password**: This check box is automatically selected after you specify an initial root password. You must clear this check box to enable the **Password** and **Verify Password** fields and specify a new password. - **Password**: The root password for the virtual machine. Enter the password in this text field and the **Verify Password** text field to verify the password. - **SSH Authorized Keys**: SSH keys to be added to the authorized keys file of the virtual machine. You can specify multiple SSH keys by entering each SSH key on a new line. - **Regenerate SSH Keys**: Regenerates SSH keys for the virtual machine.

Field Name	Operating System	Description
Custom Locale	Windows	Custom locale options for the virtual machine. Locales must be in a format such as **en-US**. Click the disclosure arrow to display the settings for this option. - **Input Locale**: The locale for user input. - **UI Language**: The language used for user interface elements such as buttons and menus. - **System Locale**: The locale for the overall system. - **User Locale**: The locale for users.
Networks	Linux	Network-related settings for the virtual machine. Click the disclosure arrow to display the settings for this option. - **DNS Servers**: The DNS servers to be used by the virtual machine. - **DNS Search Domains**: The DNS search domains to be used by the virtual machine. - **Network**: Configures network interfaces for the virtual machine. Select this check box and click **+** or **-** to add or remove network interfaces to or from the virtual machine. When you click **+**, a set of fields becomes visible that can specify whether to use DHCP, and configure an IP address, netmask, and gateway, and specify whether the network interface will start on boot.
Custom Script	Linux	Custom scripts that will be run on the virtual machine when it starts. The scripts entered in this field are custom YAML sections that are added to those produced by the Manager, and allow you to automate tasks such as creating users and files, configuring **yum** repositories and running commands. For more information on the format of scripts that can be entered in this field, see the Custom Script documentation.
Sysprep	Windows	A custom Sysprep definition. The definition must be in the format of a complete unattended installation answer file. You can copy and paste the default answer files in the **/usr/share/ovirt-engine/conf/sysprep/** directory on the machine on which the Red Hat Enterprise Virtualization Manager is installed and alter the fields as required.

4.4.4. Virtual Machine Console Settings Explained

The following table details the options available on the **Console** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.5. Virtual Machine: Console Settings

Field Name	Description
Protocol	Defines which display protocol to use. **SPICE** is the recommended protocol for Linux and Windows virtual machines, excepting Windows 8 and Windows Server 2012. Optionally, select **VNC** for Linux virtual machines. A VNC client is required to connect to a virtual machine using the VNC protocol.
VNC Keyboard Layout	Defines the keyboard layout for the virtual machine. This option is only available when using the VNC protocol.
USB Support	Defines whether USB devices can be used on the virtual machine. This option is only available for virtual machines using the SPICE protocol. Select either: - **Disabled** - Does not allow USB redirection from the client machine to the virtual machine. - **Legacy** - Enables the SPICE USB redirection policy used in Red Hat Enterprise Virtualization 3.0. This option can only be used on Windows virtual machines, and will not be supported in future versions of Red Hat Enterprise Virtualization. - **Native** - Enables native KVM/SPICE USB redirection for Linux and Windows virtual machines. Virtual machines do not require any in-guest agents or drivers for native USB. This option can only be used if the virtual machine's cluster compatibility version is set to 3.1 or higher.
Monitors	The number of monitors for the virtual machine. This option is only available for virtual desktops using the SPICE display protocol. You can choose **1**, **2** or **4**. Since Windows 8 and Windows Server 2012 virtual machines do not support the SPICE protocol, they do not support multiple monitors.
Smartcard Enabled	Smart cards are an external hardware security feature, most commonly seen in credit cards, but also used by many businesses as authentication tokens. Smart cards can be used to protect Red Hat Enterprise Virtualization virtual machines. Tick or untick the check box to activate and deactivate Smart card authentication for individual virtual machines.

Field Name	Description
Disable strict user checking	Click the **Advanced Parameters** arrow and select the check box to use this option. With this option selected, the virtual machine does not need to be rebooted when a different user connects to it. By default, strict checking is enabled so that only one user can connect to the console of a virtual machine. No other user is able to open a console to the same virtual machine until it has been rebooted. The exception is that a **SuperUser** can connect at any time and replace a existing connection. When a **SuperUser** has connected, no normal user can connect again until the virtual machine is rebooted. Disable strict checking with caution, because you can expose the previous user's session to the new user.
Soundcard Enabled	A sound card device is not necessary for all virtual machine use cases. If it is for yours, enable a sound card here.
VirtIO Console Device Enabled	The VirtIO console device is a console over VirtIO transport for communication between the host user space and guest user space. It has two parts: device emulation in QEMU that presents a virtio-pci device to the guest, and a guest driver that presents a character device interface to user space applications. Tick the check box to attach a VirtIO console device to your virtual machine.
Enable SPICE clipboard copy and paste	Defines whether a user is able to copy and paste content from an external host into the virtual machine's SPICE console. This option is only available for virtual machines using the SPICE protocol. This check box is selected by default.

4.4.5. Virtual Machine Host Settings Explained

The following table details the options available on the **Host** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.6. Virtual Machine: Host Settings

Field Name	Description

Field Name	Description
Start Running On	Defines the preferred host on which the virtual machine is to run. Select either: - **Any Host in Cluster** - The virtual machine can start and run on any available host in the cluster. - **Specific** - The virtual machine will start running on a particular host in the cluster. However, the Manager or an administrator can migrate the virtual machine to a different host in the cluster depending on the migration and high-availability settings of the virtual machine. Select the specific host from the drop-down list of available hosts.
Migration Options	Defines options to run and migrate the virtual machine. If the options here are not used, the virtual machine will run or migrate according to its cluster's policy. - **Allow manual and automatic migration** - The virtual machine can be automatically migrated from one host to another in accordance with the status of the environment, or manually by an administrator. - **Allow manual migration only** - The virtual machine can only be migrated from one host to another manually by an administrator. - **Do not allow migration** - The virtual machine cannot be migrated, either automatically or manually. The **Use Host CPU** check box allows virtual machines to take advantage of the features of the physical CPU of the host on which they are situated. This option can only be enabled when **Allow manual migration only** or **Do not allow migration** are selected. The **Use custom migration downtime** check box allows you to specify the maximum number of milliseconds the virtual machine can be down during live migration. Configure different maximum downtimes for each virtual machine according to its workload and SLA requirements. The VDSM default value is 0.

4.4.6. Virtual Machine High Availability Settings Explained

The following table details the options available on the **High Availability** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.7. Virtual Machine: High Availability Settings

Field Name	Description
Highly Available	Select this check box if the virtual machine is to be highly available. For example, in cases of host maintenance or failure, the virtual machine is automatically moved to or re-launched on another host. If the host is manually shut down by the system administrator, the virtual machine is not automatically moved to another host. Note that this option is unavailable if the **Migration Options** setting in the **Hosts** tab is set to either **Allow manual migration only** or **No migration**. For a virtual machine to be highly available, it must be possible for the Manager to migrate the virtual machine to other available hosts as necessary.
Priority for Run/Migration queue	Sets the priority level for the virtual machine to be migrated or restarted on another host.
Watchdog	Allows users to attach a watchdog card to a virtual machine. A watchdog is a timer that is used to automatically detect and recover from failures. Once set, a watchdog timer continually counts down to zero while the system is in operation, and is periodically restarted by the system to prevent it from reaching zero. If the timer reaches zero, it signifies that the system has been unable to reset the timer and is therefore experiencing a failure. Corrective actions are then taken to address the failure. This functionality is especially useful for servers that demand high availability. **Watchdog Model**: The model of watchdog card to assign to the virtual machine. At current, the only supported model is **i6300esb**. **Watchdog Action**: The action to take if the watchdog timer reaches zero. The following actions are available: - **none** - No action is taken. However, the watchdog event is recorded in the audit log. - **reset** - The virtual machine is reset and the Manager is notified of the reset action. - **poweroff** - The virtual machine is immediately shut down. - **dump** - A dump is performed and the virtual machine is paused. - **pause** - The virtual machine is paused, and can be resumed by users.

4.4.7. Virtual Machine Resource Allocation Settings Explained

The following table details the options available on the **Resource Allocation** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.8. Virtual Machine: Resource Allocation Settings

Field Name	Sub-element	Description
CPU Allocation	**CPU Profile**	The CPU profile assigned to the virtual machine. CPU profiles define the maximum amount of processing capability a virtual machine can access on the host on which it runs, expressed as a percent of the total processing capability available to that host. CPU profiles are defined on the cluster level based on quality of service entries created for data centers.
	CPU Shares	Allows users to set the level of CPU resources a virtual machine can demand relative to other virtual machines. - **Low** - 512 - **Medium** - 1024 - **High** - 2048 - **Custom** - A custom level of CPU shares defined by the user.

Field Name	Sub-element	Description
	CPU Pinning topology	Enables the virtual machine's virtual CPU (vCPU) to run on a specific physical CPU (pCPU) in a specific host. This option is not supported if the virtual machine's cluster compatibility version is set to 3.0. The syntax of CPU pinning is **v#p[_v#p]**, for example: - **0#0** - Pins vCPU 0 to pCPU 0. - **0#0_1#3** - Pins vCPU 0 to pCPU 0, and pins vCPU 1 to pCPU 3. - **1#1-4,^2** - Pins vCPU 1 to one of the pCPUs in the range of 1 to 4, excluding pCPU 2. In order to pin a virtual machine to a host, you must select **Do not allow migration** under **Migration Options**, and select the **Use Host CPU** check box.
Memory Allocation		The amount of physical memory guaranteed for this virtual machine.
Storage Allocation		The **Template Provisioning** option is only available when the virtual machine is created from a template.
	Thin	Provides optimized usage of storage capacity. Disk space is allocated only as it is required.
	Clone	Optimized for the speed of guest read and write operations. All disk space requested in the template is allocated at the time of the clone operation.
	VirtIO-SCSI Enabled	Allows users to enable or disable the use of VirtIO-SCSI on the virtual machines.

4.4.8. Virtual Machine Boot Options Settings Explained

The following table details the options available on the **Boot Options** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows

Table 4.9. Virtual Machine: Boot Options Settings

Field Name	Description
First Device	After installing a new virtual machine, the new virtual machine must go into Boot mode before powering up. Select the first device that the virtual machine must try to boot: - **Hard Disk** - **CD-ROM** - **Network (PXE)**
Second Device	Select the second device for the virtual machine to use to boot if the first device is not available. The first device selected in the previous option does not appear in the options.
Attach CD	If you have selected **CD-ROM** as a boot device, tick this check box and select a CD-ROM image from the drop-down menu. The images must be available in the ISO domain.

4.4.9. Virtual Machine Random Generator Settings Explained

The following table details the options available on the **Random Generator** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.10. Virtual Machine: Random Generator

Field Name	Description
Random Generator enabled	Selecting this check box enables a paravirtualized Random Number Generator PCI device (virtio-rng). This device allows entropy to be passed from the host to the virtual machine in order to generate a more sophisticated random number. Note that this check box can only be selected if the RNG device exists on the host and is enabled in the host's cluster.
Period duration (ms)	Specifies the duration of a period in milliseconds. If omitted, the libvirt default of 1000 milliseconds (1 second) is used. If this field is filled, **Bytes per period** must be filled also.
Bytes per period	Specifies how many bytes are permitted to be consumed per period.
Device source:	The source of the random number generator. This is automatically selected depending on the source supported by the host's cluster. - **/dev/random source** - The Linux-provided random number generator. - **/dev/hwrng source** - An external hardware generator.

Important

This feature is only supported with a host running Red Hat Enterprise Linux 6.6 and later or Red Hat Enterprise Linux 7.0 and later.

4.4.10. Virtual Machine Custom Properties Settings Explained

The following table details the options available on the **Custom Properties** tab of the **New Virtual Machine** and **Edit Virtual Machine** windows.

Table 4.11. Virtual Machine: Custom Properties Settings

Field Name	Description	Recommendations and Limitations
sap_agent	Enables SAP monitoring on the virtual machine. Set to **true** or **false**.	-
sndbuf	Enter the size of the buffer for sending the virtual machine's outgoing data over the socket. Default value is 0.	-
vhost	Disables vhost-net, which is the kernel-based virtio network driver on virtual network interface cards attached to the virtual machine. To disable vhost, the format for this property is: `LogicalNetworkName:false` This will explicitly start the virtual machine without the vhost-net setting on the virtual NIC attached to *LogicalNetworkName*.	vhost-net provides better performance than virtio-net, and if it is present, it is enabled on all virtual machine NICs by default. Disabling this property makes it easier to isolate and diagnose performance issues, or to debug vhost-net errors; for example, if migration fails for virtual machines on which vhost does not exist.
viodiskcache	Caching mode for the virtio disk. **writethrough** writes data to the cache and the disk in parallel, **writeback** does not copy modifications from the cache to the disk, and **none** disables caching.	For Red Hat Enterprise Virtualization 3.1, if viodiskcache is enabled, the virtual machine cannot be live migrated.

Warning

Increasing the value of the sndbuf custom property results in increased occurrences of communication failure between hosts and unresponsive virtual machines.

4.5. Configuring Virtual Machines

4.5.1. Completing the Configuration of a Virtual Machine by Defining Network Interfaces and Hard Disks

Summary

Before you can use your newly created virtual machine, the **Guide Me** window prompts you to configure at least one network interface and one virtual disk for the virtual machine.

Procedure 4.6. Completing the Configuration of a Virtual Machine by Defining Network Interfaces and Hard Disks

1. On the **New Virtual Machine - Guide Me** window, click the **Configure Network Interfaces** button to open the **New Network Interface** window. You can accept the default values or change them as necessary.

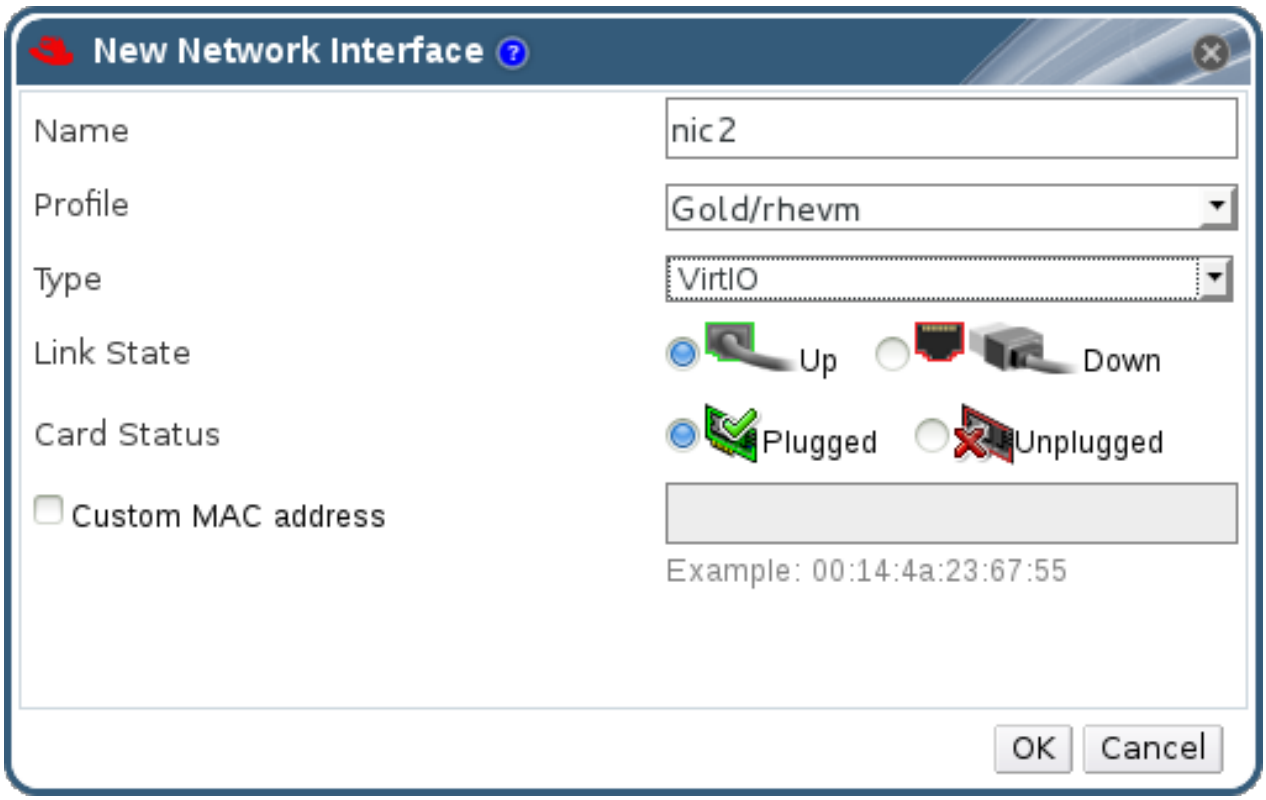


Figure 4.6. New Network Interface window

Enter the **Name** of the network interface.

2. Use the drop-down menus to select the **Network** and the **Type** of network interface for the new virtual machine. The **Link State** is set to **Up** by default when the NIC is defined on the virtual machine and connected to the network.

Note

The options on the **Network** and **Type** fields are populated by the networks available to the cluster, and the NICs available to the virtual machine.

3. If applicable, select the **Specify custom MAC address** check box and enter the network interface's MAC address.
4. Click the arrow next to **Advanced Parameters** to configure the **Port Mirroring** and **Card Status** fields, if necessary.
5. Click **OK** to close the **New Network Interface** window and open the **New Virtual Machine - Guide Me** window.
6. Click the **Configure Virtual Disk** button to open the **New Virtual Disk** window.
7. Add either an **Internal** virtual disk or an **External** LUN to the virtual machine.

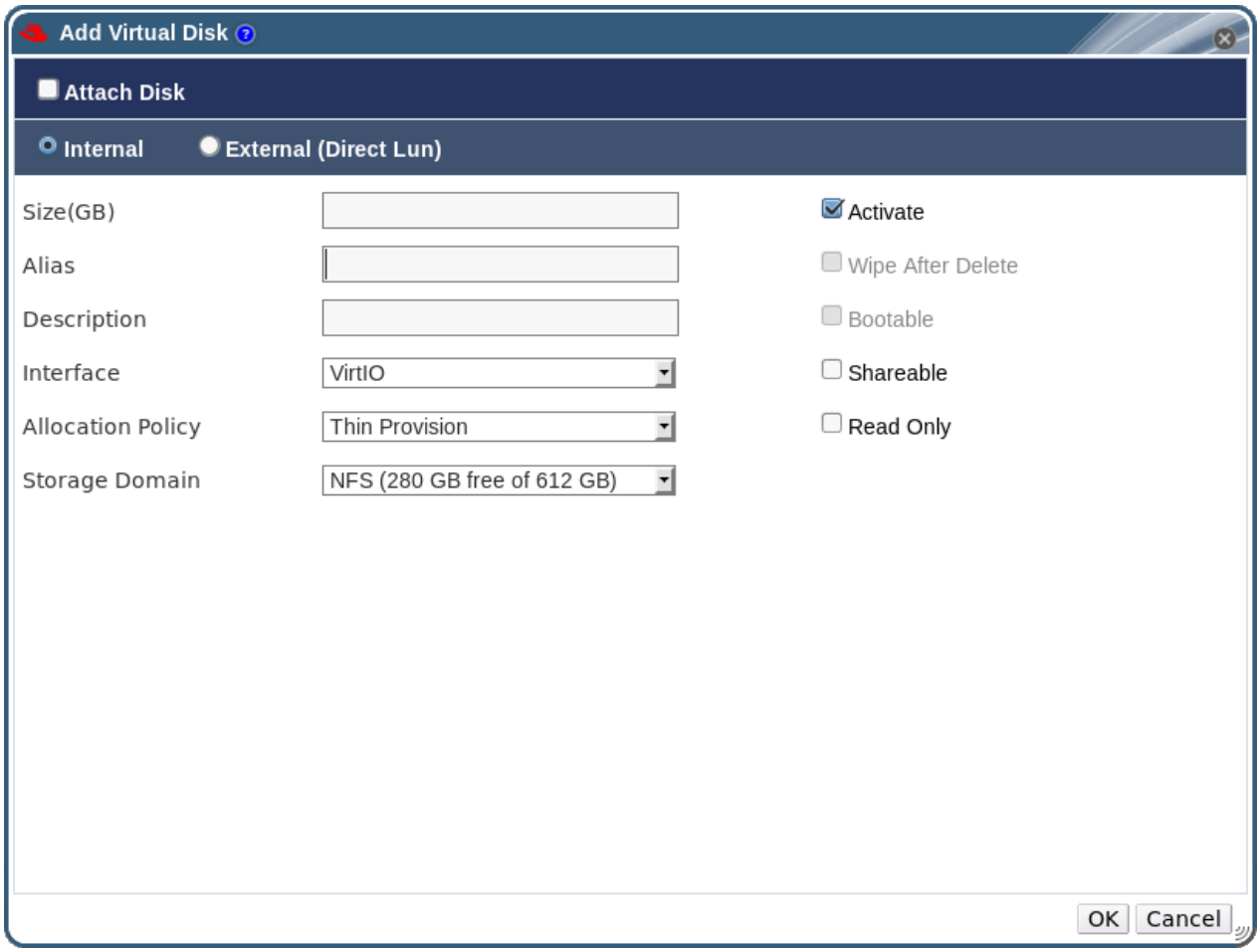


Figure 4.7. New Virtual Disk Window

8. Click **OK** to close the **New Virtual Disk** window. The **New Virtual Machine - Guide Me** window opens with changed context. There is no further mandatory configuration.
9. Click **Configure Later** to close the window.

Result

You have added a network interface and a virtual disk to your virtual machine.

4.5.2. Installing Windows on VirtIO-Optimized Hardware

Summary

The **virtio-win.vfd** diskette image contains Windows drivers for VirtIO-optimized disk and network devices. These drivers provide a performance improvement over emulated device drivers.

The **virtio-win.vfd** is placed automatically on ISO storage domains that are hosted on the Manager server. It must be manually uploaded using the **engine-iso-uploader** tool to other ISO storage domains.

You can install the VirtIO-optimized device drivers during your Windows installation by attaching a diskette to your virtual machine.

This procedure presumes that you added a **Red Hat VirtIO** network interface and a disk that uses the **VirtIO** interface to your virtual machine.

Procedure 4.7. Installing VirtIO Drivers during Windows Installation

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click the **Run Once** button, and the **Run Once** window displays.
3. Click **Boot Options** to expand the **Boot Options** configuration options.
4. Click the **Attach Floppy** check box, and select **virtio-win.vfd** from the drop down selection box.
5. Click the **Attach CD** check box, and select from the drop down selection box the ISO containing the version of Windows you want to install.
6. Move **CD-ROM UP** in the **Boot Sequence** field.
7. Configure the rest of your **Run Once** options as required, and click **OK** to start your virtual machine, and then click the **Console** button to open a graphical console to your virtual machine.

Result

Windows installations include an option to load additional drivers early in the installation process. Use this option to load drivers from the **virtio-win.vfd** diskette that was attached to your virtual machine as **A:**.

For each supported virtual machine architecture and Windows version, there is a folder on the disk containing optimized hardware device drivers.

4.5.3. Virtual Machine Run Once Settings Explained

The **Run Once** window defines one-off boot options for a virtual machine. For persistent boot options, use the **Boot Options** tab in the **New Virtual Machine** window.

Boot Options

Defines the virtual machine's boot sequence, running options, and source images for installing the operating system and required drivers.

Attach Floppy

Attaches a diskette image to the virtual machine. Use this option to install Windows drivers. The diskette image must reside in the ISO domain.

Attach CD

Attaches an ISO image to the virtual machine. Use this option to install the virtual machine's operating system and applications. The CD image must reside in the ISO domain.

Boot Sequence

Determines the order in which the boot devices are used to boot the virtual machine. Select either **Hard Disk**, **CD-ROM** or **Network**, and use **Up** and **Down** to move the option up or down in the list.

Run Stateless

Deletes all changes to the virtual machine upon shutdown. This option is only available if a virtual disk is attached to the virtual machine.

Start in Pause Mode

Starts then pauses the virtual machine to enable connection to the console, suitable for virtual machines in remote locations.

Linux Boot Options

The following options boot a Linux kernel directly instead of through the BIOS bootloader.

kernel path

A fully qualified path to a kernel image to boot the virtual machine. The kernel image must be stored on either the ISO domain (path name in the format of **iso://path-to-image**) or on the host's local storage domain (path name in the format of **/data/images**).

initrd path

A fully qualified path to a ramdisk image to be used with the previously specified kernel. The ramdisk image must be stored on the ISO domain (path name in the format of **iso://path-to-image**) or on the host's local storage domain (path name in the format of **/data/images**).

kernel params

Kernel command line parameter strings to be used with the defined kernel on boot.

Initial Run

Specifies whether to use Cloud-Init or Sysprep to initialize the virtual machine. For Linux-based virtual machines, you must select the **Use Cloud-Init** check box in the **Initial Run** tab to view the available options. For Windows-based virtual machines, you must attach the **[sysprep]** floppy by selecting the **Attach Floppy** check box in the **Boot Options** tab and selecting the floppy from the list. Certain options are only available on Linux-based or Windows-based virtual machines, as noted below.

VM Hostname

The host name of the virtual machine.

Domain

The Active Directory domain to which the virtual machine belongs. (Windows)

Organization Name

The name of the organization to which the virtual machine belongs. This option corresponds to the text field for setting the organization name displayed when a machine running Windows is started for the first time. (Windows)

Active Directory OU

The organizational unit in the Active Directory domain to which the virtual machine belongs. (Windows)

Configure Time Zone

The time zone for the virtual machine. Select this check box and select a time zone from the **Time Zone** list.

Alternate Credentials

Selecting this check box allows you to set a **User Name** and **Password** as alternative credentials. (Windows)

Admin Password

The administrative user password for the virtual machine. Click the disclosure arrow to display the settings for this option. (Windows)

Use already configured password

This check box is automatically selected after you specify an initial administrative user password. You must clear this check box to enable the **Admin Password** and **Verify Admin Password** fields and specify a new password.

Admin Password

The administrative user password for the virtual machine. Enter the password in this text field and the **Verify Admin Password** text field to verify the password.

Authentication

The authentication details for the virtual machine. Click the disclosure arrow to display the settings for this option. (Linux)

User Name

Creates a new user account on the virtual machine. If this field is not filled in, the default user is **root**.

Use already configured password

This check box is automatically selected after you specify an initial root password. You must clear this check box to enable the **Password** and **Verify Password** fields and specify a new password.

Password

The root password for the virtual machine. Enter the password in this text field and the **Verify Password** text field to verify the password.

SSH Authorized Keys

SSH keys to be added to the authorized keys file of the virtual machine.

Regenerate SSH Keys

Regenerates SSH keys for the virtual machine.

Custom Locale

Custom locale options for the virtual machine. Locales must be in a format such as **en-US**. Click the disclosure arrow to display the settings for this option. (Windows)

Input Locale

The locale for user input.

UI Language

The language used for user interface elements such as buttons and menus.

System Locale

The locale for the overall system.

User Locale

The locale for users.

Networks

Network-related settings for the virtual machine. Click the disclosure arrow to display the settings for this option. (Linux)

DNS Servers

The DNS servers to be used by the virtual machine.

DNS Search Domains

The DNS search domains to be used by the virtual machine.

Network

Configures network interfaces for the virtual machine. Select this check box and click **+** or **-** to add or remove network interfaces to or from the virtual machine. When you click **+**, a set of fields becomes visible that can specify whether to use DHCP, and configure an IP address, netmask, and gateway, and specify whether the network interface will start on boot.

Custom Script

Custom scripts that will be run on the virtual machine when it starts.

Custom Scripts

The scripts entered in this field are custom YAML sections that are added to those produced by the Manager, and allow you to automate tasks such as creating users and files, configuring **yum** repositories and running commands. For more information on the format of scripts that can be entered in this field, see the Custom Script documentation. (Linux)

Sysprep

A custom Sysprep definition.

Sysprep

The definition must be in the format of a complete unattended installation answer file. You can copy and paste the default answer files in the **/usr/share/ovirt-engine/conf/sysprep/** directory on the machine on which the Red Hat Enterprise Virtualization Manager is installed and alter the fields as required. (Windows)

Host

Defines the virtual machine's host.

Any host in cluster

Allocates the virtual machine to any available host.

Specific

Specifies a user-defined host for the virtual machine.

Display Protocol

Defines the protocol to connect to virtual machines.

VNC

Can be used for Linux virtual machines. Requires a VNC client to connect to a virtual machine using VNC. Optionally, specify **VNC Keyboard Layout** from the drop-down list.

SPICE

Recommended protocol for Linux and Windows virtual machines, excepting Windows 8 and Server 2012 virtual machines.

Custom Properties

Additional VDSM options for running virtual machines.

sap_agent

Enables SAP monitoring on the virtual machine. Set to **true** or **false**.

sndbuf

Enter the size of the buffer for sending the virtual machine's outgoing data over the socket.

vhost

Enter the name of the virtual host on which this virtual machine should run. The name can contain any combination of letters and numbers.

viodiskcache

Caching mode for the virtio disk. **writethrough** writes data to the cache and the disk in parallel, **writeback** does not copy modifications from the cache to the disk, and **none** disables caching.

4.5.4. Configuring a Watchdog

4.5.4.1. Adding a Watchdog Card to a Virtual Machine

Summary

Add a watchdog card to a virtual machine.

Procedure 4.8. Adding a Watchdog Card to a Virtual Machine

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click **Edit** to open the **Edit Virtual Machine** window.
3. Click **Show Advanced Options** to display all tabs and click the **High Availability** tab.
4. Select the watchdog model to use from the **Watchdog Model** drop-down menu.
5. Select an action from the **Watchdog Action** drop-down menu. This is the action that the virtual machine takes when the watchdog is triggered.
6. Click **OK**.

Result

You have added a watchdog card to the virtual machine.

4.5.4.2. Installing a Watchdog

Summary

To activate a watchdog card attached to a virtual machine, you must install the *watchdog* package on that virtual machine and start the **watchdog** service.

Procedure 4.9. Installing a Watchdog

1. Log on to the virtual machine on which the watchdog card is attached.
2. Run the following command to install the *watchdog* package and dependencies:

```
# yum install watchdog
```

3. Edit the **/etc/watchdog.conf** file and uncomment the following line:

```
watchdog-device = /dev/watchdog
```

4. Save the changes.
5. Run the following commands to start the **watchdog** service and ensure this service starts on boot:

```
# service watchdog start
# chkconfig watchdog on
```

Result

You have installed and started the **watchdog** service on a virtual machine.

4.5.4.3. Confirming Watchdog Functionality

Summary

Confirm that a watchdog card has been attached to a virtual machine and that the **watchdog** service is active.

Warning

This procedure is provided for testing the functionality of watchdogs only and must not be run on production machines.

Procedure 4.10. Confirming Watchdog Functionality

1. Log on to the virtual machine on which the watchdog card is attached.
2. Run the following command to confirm that the watchdog card has been identified by the virtual machine:

```
# lspci | grep watchdog -i
```

3. Run one of the following commands to confirm that the watchdog is active:
   - Run the following command to trigger a kernel panic:

```
# echo c > /proc/sysrq-trigger
```

   - Run the following command to terminate the **watchdog** service:

```
# kill -9 `pgrep watchdog`
```

Result

The watchdog timer can no longer be reset, so the watchdog counter reaches zero after a short period of time. When the watchdog counter reaches zero, the action specified in the **Watchdog Action** drop-down menu for that virtual machine is performed.

4.5.4.4. Parameters for Watchdogs in watchdog.conf

The following is a list of options for configuring the **watchdog** service available in the **/etc/watchdog.conf** file. To configure an option, you must ensure that option is uncommented and restart the **watchdog** service after saving the changes.

Note

For a more detailed explanation of options for configuring the **watchdog** service and using the **watchdog** command, see the **watchdog** man page.

Table 4.12. watchdog.conf variables

Variable name	Default Value	Remarks
ping	N/A	An IP address that the watchdog attempts to ping to verify whether that address is reachable. You can specify multiple IP addresses by adding additional **ping** lines.
interface	N/A	A network interface that the watchdog will monitor to verify the presence of network traffic. You can specify multiple network interfaces by adding additional **interface** lines.
file	**/var/log/messages**	A file on the local system that the watchdog will monitor for changes. You can specify multiple files by adding additional **file** lines.
change	**1407**	The number of watchdog intervals after which the watchdog checks for changes to files. A **change** line must be specified on the line directly after each **file** line, and applies to the **file** line directly above that **change** line.
max-load-1	**24**	The maximum average load that the virtual machine can sustain over a one-minute period. If this average is exceeded, then the watchdog is triggered. A value of **0** disables this feature.
max-load-5	**18**	The maximum average load that the virtual machine can sustain over a five-minute period. If this average is exceeded, then the watchdog is triggered. A value of **0** disables this feature. By default, the value of this variable is set to a value approximately three quarters that of **max-load-1**.
max-load-15	**12**	The maximum average load that the virtual machine can sustain over a fifteen-minute period. If this average is exceeded, then the watchdog is triggered. A value of **0** disables this feature. By default, the value of this variable is set to a value approximately one half that of **max-load-1**.

Variable name	Default Value	Remarks
min-memory	**1**	The minimum amount of virtual memory that must remain free on the virtual machine. This value is measured in pages. A value of **0** disables this feature.
repair-binary	**/usr/sbin/repair**	The path and file name of a binary file on the local system that will be run when the watchdog is triggered. If the specified file resolves the issues preventing the watchdog from resetting the watchdog counter, then the watchdog action is not triggered.
test-binary	N/A	The path and file name of a binary file on the local system that the watchdog will attempt to run during each interval. A test binary allows you to specify a file for running user-defined tests.
test-timeout	N/A	The time limit, in seconds, for which user-defined tests can run. A value of **0** allows user-defined tests to continue for an unlimited duration.
temperature-device	N/A	The path to and name of a device for checking the temperature of the machine on which the **watchdog** service is running.
max-temperature	**120**	The maximum allowed temperature for the machine on which the **watchdog** service is running. The machine will be halted if this temperature is reached. Unit conversion is not taken into account, so you must specify a value that matches the watchdog card being used.
admin	**root**	The email address to which email notifications are sent.
interval	**10**	The interval, in seconds, between updates to the watchdog device. The watchdog device expects an update at least once every minute, and if there are no updates over a one-minute period, then the watchdog is triggered. This one-minute period is hard-coded into the drivers for the watchdog device, and cannot be configured.
logtick	**1**	When verbose logging is enabled for the **watchdog** service, the **watchdog** service periodically writes log messages to the local system. The **logtick** value represents the number of watchdog intervals after which a message is written.

Variable name	Default Value	Remarks
realtime	**yes**	Specifies whether the watchdog is locked in memory. A value of **yes** locks the watchdog in memory so that it is not swapped out of memory, while a value of **no** allows the watchdog to be swapped out of memory. If the watchdog is swapped out of memory and is not swapped back in before the watchdog counter reaches zero, then the watchdog is triggered.
priority	**1**	The schedule priority when the value of **realtime** is set to **yes**.
pidfile	**/var/run/syslogd.pid**	The path and file name of a PID file that the watchdog monitors to see if the corresponding process is still active. If the corresponding process is not active, then the watchdog is triggered.

4.6. Editing Virtual Machines

4.6.1. Editing Virtual Machine Properties

Summary

Changes to storage, operating system, or networking parameters can adversely affect the virtual machine. Ensure that you have the correct details before attempting to make any changes. Virtual machines can be edited while running, and some changes (listed in the procedure below) will be applied immediately. To apply all changes, the virtual machine must be restarted or shut down.

Procedure 4.11. Editing a virtual machine:

1. Select the virtual machine to be edited.
2. Click the **Edit** button to open the **Edit Virtual Machine** window.
3. Change the **General**, **System**, **Initial Run**, **Console**, **Host**, **High Availability**, **Resource Allocation**, **Boot Options**, **Random Generator**, and **Custom Properties** fields as required.

   Changes to the following fields are applied immediately:

   - **Name**
   - **Description**
   - **Comment**
   - **Optimized for** (Desktop/Server)
   - **Delete Protection**
   - **Network Interfaces**
   - **Use custom migration downtime**

- **Highly Available**
- **Priority for Run/Migration queue**
- **Disable strict user checking**
- **Virtual Sockets** (Tech preview, on supported guest operating systems only.)

To apply changes to all other settings, the virtual machine must be restarted or shut down.

4. If the **Next Restart Configuration** pop-up window appears, click **OK**.
5. Click **OK** to save your changes. Changes from the list in Step 3 will be applied immediately. All other changes will be applied once you restart your virtual machine.

Result

You have changed the settings of a virtual machine by editing it.

4.6.2. Editing a Network Interface

Summary

This procedure describes editing a network interface. In order to change any network settings, you must edit the network interface.

Procedure 4.12. Editing a Network Interface

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click the **Network Interfaces** tab of the details pane and select the network interface to edit.
3. Click **Edit** to open the **Edit Network Interface** window. This dialog contains the same fields as the **New Network Interface** dialog.
4. Click **OK** to save your changes once you are finished.

Result

You have now changed the network interface by editing it.

4.6.3. Extending the Size of an Online Virtual Disk

Summary

This procedure explains how to extend the size of a virtual drive while the virtual drive is attached to a virtual machine.

Procedure 4.13. Extending the Size of an Online Virtual Disk

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Select the **Disks** tab in the details pane.
3. Select a target disk from the list in the details pane.
4. Click **Edit** in the details pane.

5. Enter a value in the **Extend size by(GB)** field.
6. Click **OK**.

Result

The target disk's status becomes **locked** for a short time, during which the drive is resized. When the resizing of the drive is complete, the status of the drive becomes **OK**.

4.6.4. Floating Disks

Floating disks are disks that are not associated with any virtual machine.

Floating disks can minimize the amount of time required to set up virtual machines. Designating a floating disk as storage for a VM makes it unnecessary to wait for disk preallocation at the time of a VM's creation.

Floating disks can be attached to virtual machines or designated as shareable disks, which can be used with one or more VMs.

4.6.5. Associating a Virtual Disk with a Virtual Machine

Summary

This procedure explains how to associate a virtual disk with a virtual machine. Once the virtual disk is associated with the virtual machine, the VM is able to access it.

Procedure 4.14. Associating a Virtual Disk with a Virtual Machine

1. Click the **Virtual Machines** tab and select a virtual machine.
2. In the details pane, select the **Disks** tab.
3. Click **Add** in the menu at the top of the Details Pane.
4. Type the size in GB of the disk into the **Size(GB)** field.
5. Type the disk alias into the **Alias** field.
6. Click **OK** in the bottom right corner of the **Add Virtual Disk** window.

   The disk you have associated with the virtual machine appears in the details pane after a short time.

Result

The virtual disk is associated with the virtual machine.

Note

No Quota resources are consumed by attaching virtual disks to, or detaching virtual disks from, virtual machines.

Note

Using the above procedure, it is now possible to attach a virtual disk to more than one virtual machine.

4.6.6. Changing the CD for a Virtual Machine

Summary

You can change the CD accessible to a virtual machine while that virtual machine is running.

Note

You can only use ISO files that have been added to the ISO domain of the cluster in which the virtual machine is a member. Therefore, you must upload ISO files to that domain before you can make those ISO files accessible to virtual machines.

Procedure 4.15. Changing the CD for a Virtual Machine

1. From the **Virtual Machines** tab, select a virtual machine that is currently running.
2. Click **Change CD** to open the **Change CD** window.
3. In the **Change CD** window do one of the following:
   - Select an ISO file from the list to eject the CD currently accessible to the virtual machine and mount that ISO file as a CD.

     Or,

   - Select **[Eject]** from the ISO list to eject the CD currently accessible to the virtual machine.
4. Click **OK**.

Result

You have ejected the CD previously accessible to the virtual machine, or ejected the CD previously accessible to the virtual machine and made a new CD accessible to that virtual machine

4.6.7. Smart card Authentication

Smart cards are an external hardware security feature, most commonly seen in credit cards, but also used by many businesses as authentication tokens. Smart cards can be used to protect Red Hat Enterprise Virtualization virtual machines.

4.6.8. Enabling and Disabling Smart cards

Summary

The following procedures explain how to enable and disable the Smart card feature for virtual machines.

Procedure 4.16. Enabling Smart cards

1. Ensure that the Smart card hardware is plugged into the client machine and is installed according to manufacturer's directions.
2. Select the desired virtual machine.
3. Click the **Edit** button. The **Edit Virtual Machine** window appears.
4. Select the **Console** tab, and select the check box labeled **Smartcard enabled**, then click **OK**.
5. Run the virtual machine by clicking the **Console** icon or through the User Portal. Smart card authentication is now passed from the client hardware to the virtual machine.

Result

You have enabled Smart card authentication for the virtual machine.

Important

If the Smart card hardware is not correctly installed, enabling the Smart card feature will result in the virtual machine failing to load properly.

Procedure 4.17. Disabling Smart cards

1. Select the desired virtual machine.
2. Click the **Edit** button. The **Edit Virtual Machine** window appears.
3. Select the **Console** tab, and clear the check box labeled **Smartcard enabled**, then click **OK**.

Result

You have disabled Smart card authentication for the virtual machine.

4.7. Removing Virtual Machines

4.7.1. Removing a Virtual Machine

Summary

Remove a virtual machine from the Red Hat Enterprise Virtualization environment.

Important

The **Remove** button is disabled while virtual machines are running; you must shut down a virtual machine before you can remove it.

Procedure 4.18. Removing a Virtual Machine

1. Click the **Virtual Machines** tab and select the virtual machine to remove.
2. Click **Remove** to open the **Remove Virtual Machine(s)** window.
3. Optionally, select the **Remove Disk(s)** check box to remove the virtual disks attached to the virtual machine together with the virtual machine. If the **Remove Disk(s)** check box is cleared, then the virtual disks remain in the environment as floating disks.
4. Click **OK**.

Result

The virtual machine is removed from the environment and is no longer listed in the **Virtual Machines** resource tab. If you selected the **Remove Disk(s)** check box, then the virtual disks attached to the virtual machine are also removed.

4.8. Cloning Virtual Machines

4.8.1. Cloning a Virtual Machine

Summary

In Red Hat Enterprise Virtualization 3.5, you can now clone virtual machines without having to create a template or a snapshot first.

Important

The **Clone VM** button is disabled while virtual machines are running; you must shut down a virtual machine before you can clone it.

Procedure 4.19. Cloning a Virtual Machine

1. Click the **Virtual Machines** tab and select the virtual machine to clone.
2. Click the **Clone VM** button to open the **Clone Virtual Machine** window.
3. Enter a name for the new virtual machine.
4. Click **OK**.

Result

A duplicate virtual machine is generated.

4.9. Snapshots

4.9.1. Managing Snapshots

Before you make changes to your virtual machine, it is recommended to use snapshots to back up all the virtual machine's existing data. A snapshot displays a view of the virtual machine's operating system and all its applications at a given point in time, and can be used to restore a virtual machine to a previous state.

Important

Live snapshots can only be taken on Data Centers running Red Hat Enterprise Virtualization 3.1 or higher. Otherwise, the virtual machine must first be powered down.

4.9.2. Creating Snapshots

Summary

This procedure explains how to create a snapshot of a virtual machine.

Procedure 4.20. Creating a snapshot of a virtual machine

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Select the **Snapshots** tab in the details pane.
3. Click **Create**. The **Create Snapshot** dialog displays.
4. Enter a description for the snapshot, select **Disks to include** using the check boxes. and click **OK**.
5. A new snapshot of the virtual machine's operating system and applications is created. It displays in a list on the left side of the **Snapshots** tab.

Result

You have taken a snapshot of a virtual machine.

4.9.3. Cloning Snapshots

Summary

This procedure explains how to clone a virtual machine from a snapshot.

Procedure 4.21. Cloning Snapshots

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Select the **Snapshots** tab in the details pane.
3. Select the snapshot from which to create a clone in the list in the details pane.
4. Click **Clone** at the top of the details pane.

   The **Clone VM from Snapshot** window opens. This window is similar to the **New VM** window.
5. Fill in the parameters and click **OK** in the lower-right corner of the **Clone VM from Snapshot** window.

Result

You have cloned a virtual machine from a snapshot.

4.9.4. Using a Snapshot to Restore a Virtual Machine

4.9.4. Using a Snapshot to Restore a Virtual Machine

Summary

A snapshot can be used to restore a virtual machine to its previous state.

Procedure 4.22. Using a snapshot to restore a virtual machine

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click the **Snapshots** tab in the details pane to list the available snapshots.
3. Select a snapshot to restore in the left side-pane. The snapshot details display in the right side-pane.
4. Click the drop-down list beside **Preview** to open the **Custom Preview Snapshot** window.

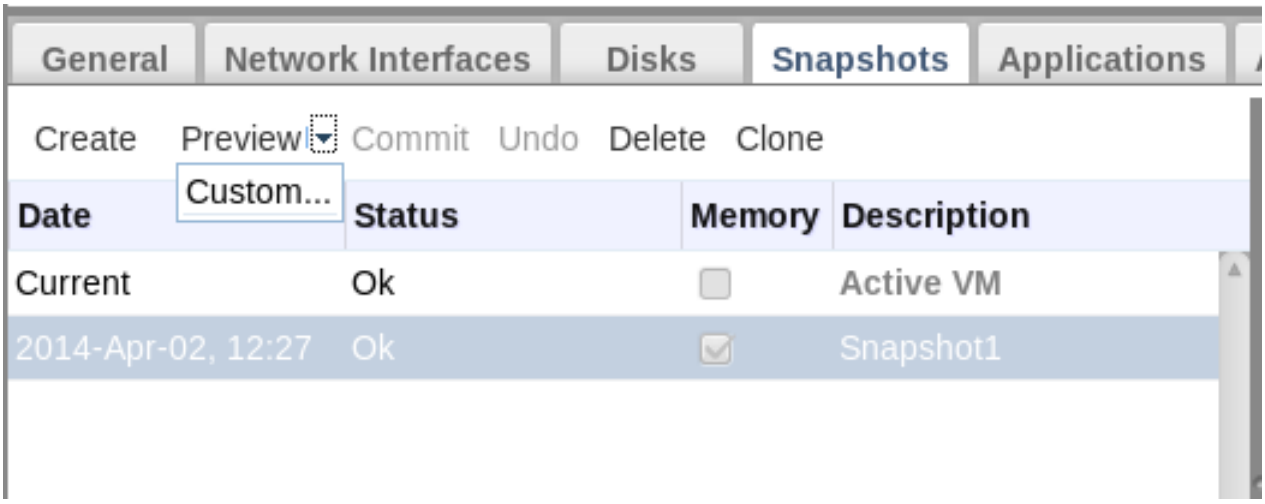


Figure 4.8. Custom preview snapshot

5. Use the check boxes to select the **VM Configuration**, **Memory**, and disk(s) you want to restore, then click **OK**. This allows you to create and restore from a customized snapshot using the configuration and disk(s) from multiple snapshots.

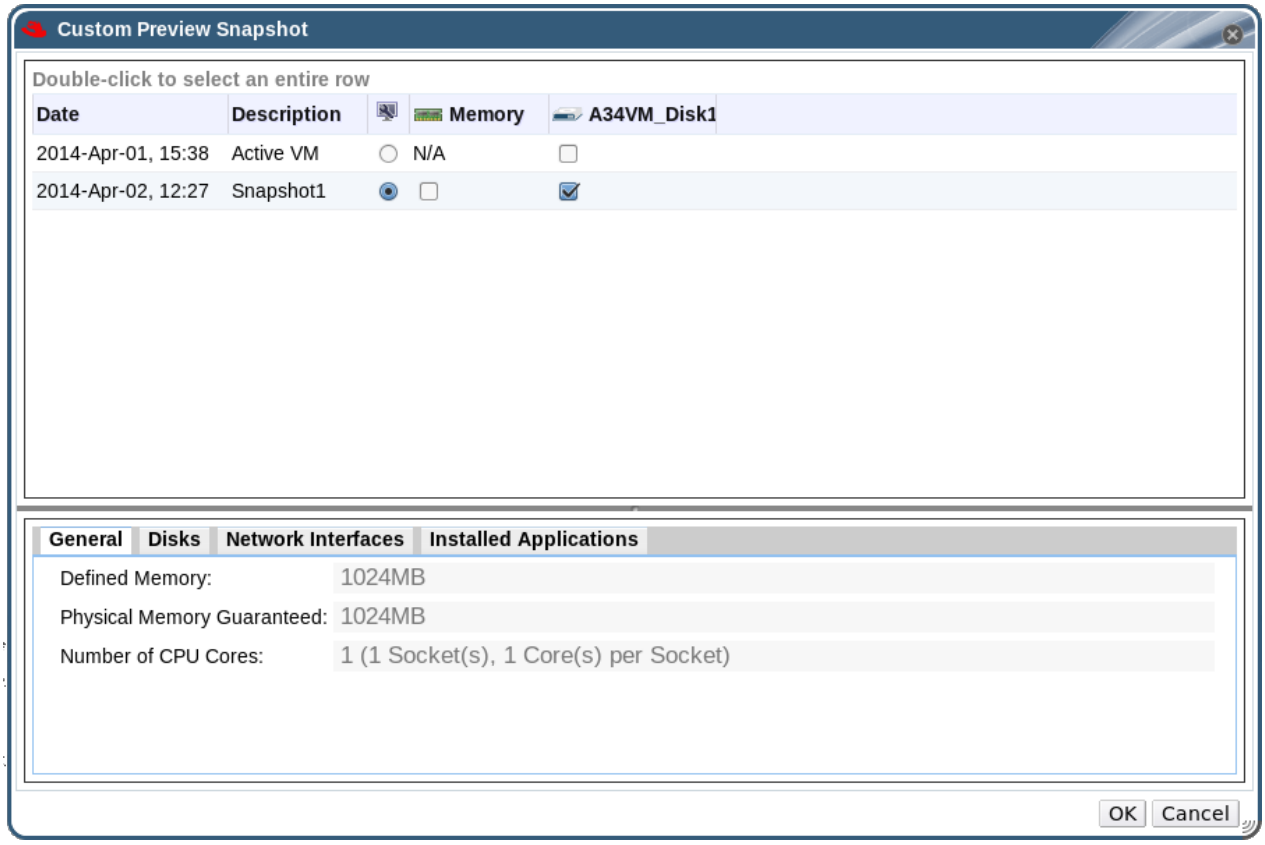


Figure 4.9. Custom preview snapshot

The status of the snapshot changes to **Preview Mode**. The status of the virtual machine briefly changes to **Image Locked** before returning to **Down**.

6. Start the virtual machine; it runs using the disk image of the snapshot.
7. Click **Commit** to permanently restore the virtual machine to the condition of the snapshot. Any subsequent snapshots are erased.

   Alternatively, click the **Undo** button to deactivate the snapshot and return the virtual machine to its previous state.

Result

The virtual machine is restored to its state at the time of the snapshot, or returned to its state before the preview of the snapshot.

4.9.5. Deleting a Snapshot

Summary

Delete a virtual machine snapshot and permanently remove it from your Red Hat Enterprise Virtualization environment.

Important

When you delete a snapshot, a new logical volume is created of the same size as the snapshot. The snapshot being deleted is then merged with the subsequent snapshot in the new volume; the new volume is extended to accommodate the total size of the two merged snapshots. If there is no data overlap between the two merged snapshots, the new logical volume size will be the sum of the two merged snapshots. To delete a snapshot, you must therefore have at least the same amount of free storage space as the total size of the snapshot being deleted and the subsequent snapshot.

Procedure 4.23. Deleting a Snapshot

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click the **Snapshots** tab in the details pane to list the snapshots for that virtual machine.

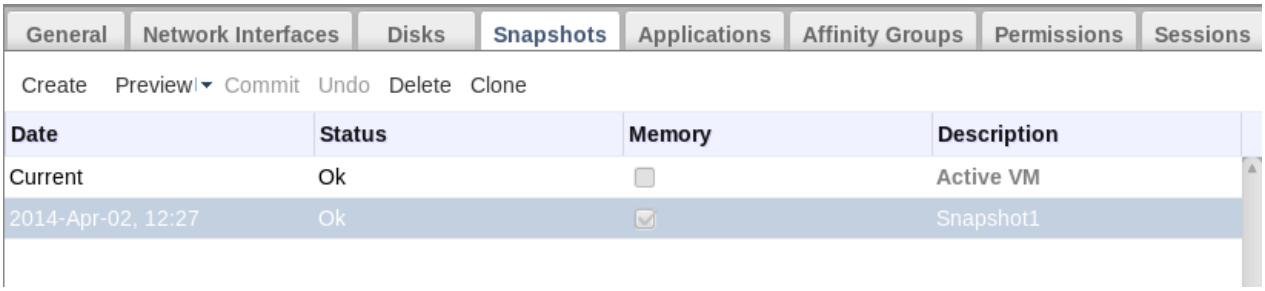


Figure 4.10. Snapshot List

3. Select the snapshot to delete.
4. In the Navigation pane, shut down the running virtual machine associated with the snapshot to be deleted.
5. Click **Delete** to open the **Delete Snapshot** confirmation window.
6. Click **OK**.

Result

You have removed a snapshot from a virtual machine, and that snapshot is no longer available.

4.10. Templates

4.10.1. Introduction to Templates

A template is a copy of a virtual machine that you can use to simplify the subsequent, repeated creation of similar virtual machines. Templates capture the configuration of software, configuration of hardware, and the software installed on the virtual machine on which the template is based. The virtual machine on which a template is based is known as the source virtual machine.

When you create a template based on a virtual machine, a read-only copy of the virtual machine's disk is created. This read-only disk becomes the base disk image of the new template, and of any virtual machines created based on the template. As such, the template cannot be deleted while any virtual machines created based on the template exist in the environment.

Virtual machines created based on a template use the same NIC type and driver as the original virtual machine, but are assigned separate, unique MAC addresses.

4.10.2. Template Tasks

4.10.2.1. Creating a Template

Summary

Create a template from an existing virtual machine to use as a blueprint for creating additional virtual machines.

Important

Before you create a template, you must seal the source virtual machine to ensure all system-specific details are removed from the virtual machine. This is necessary to prevent the same details from appearing on multiple virtual machines created based on the same template.

Procedure 4.24. Creating a Template

1. Click the **Virtual Machines** tab.
2. Select the source virtual machine.
3. Ensure the virtual machine is powered down and has a status of **Down**.
4. Click **Make Template**.

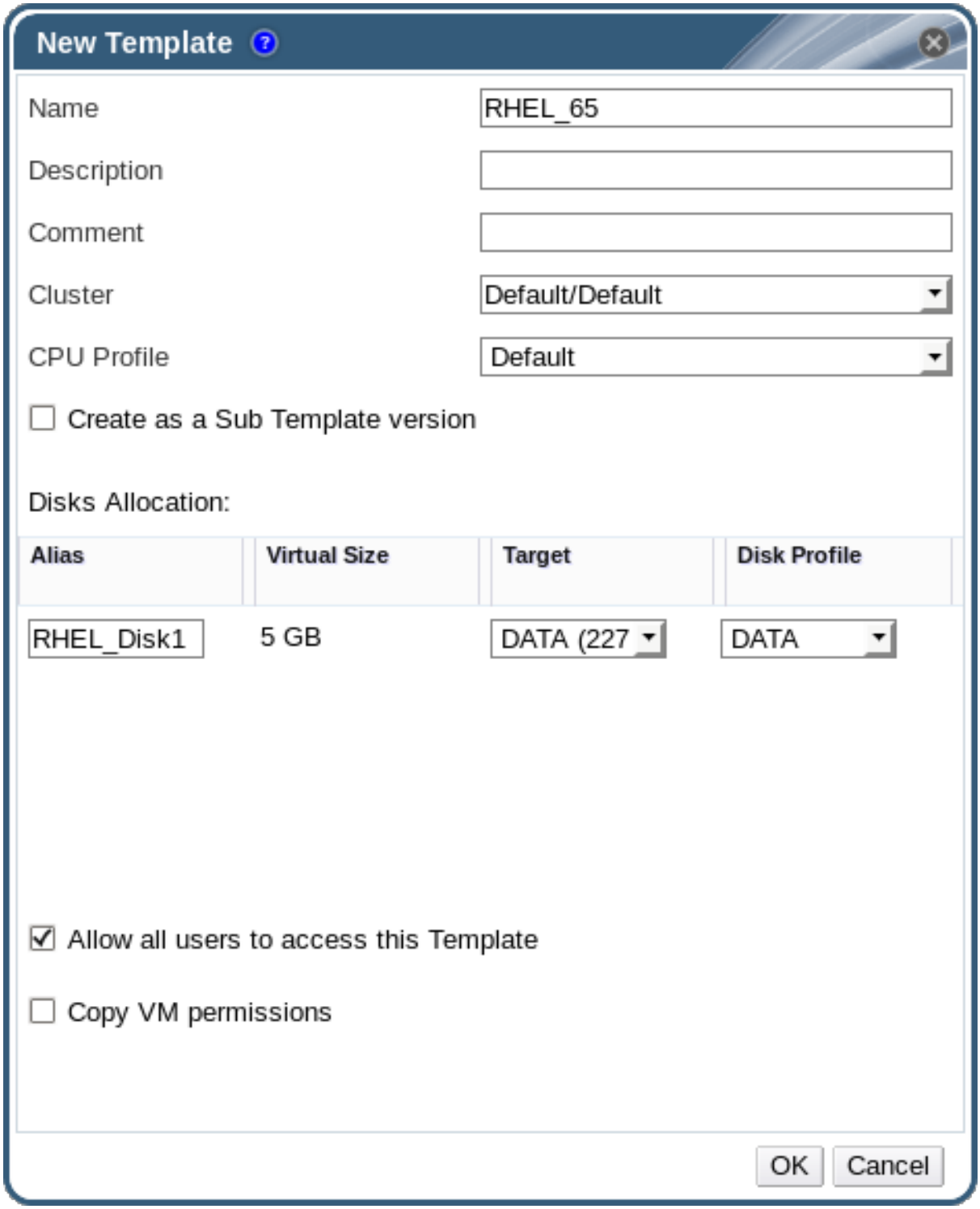


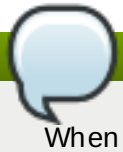
Figure 4.11. The New Template window

5. Enter a **Name**, **Description**, and **Comment** for the template.
6. Select the cluster with which to associate the template from the **Cluster** list. By default, this is the same as that of the source virtual machine.
7. Optionally, select a CPU profile for the template from the **CPU Profile** list.
8. Optionally, select the **Create as a Sub Template version** check box, select a **Root Template**, and enter a **Sub Version Name** to create the new template as a sub template of an existing template.

9. In the **Disks Allocation** section, enter an alias for the disk in the **Alias** text field, and select the storage domain on which to store the disk from the **Target** list. By default, these are the same as those of the source virtual machine.
10. Select the **Allow all users to access this Template** check box to make the template public.
11. Select the **Copy VM permissions** check box to copy the permissions of the source virtual machine to the template.
12. Click **OK**.

Result

The virtual machine displays a status of **Image Locked** while the template is being created. The process of creating a template may take up to an hour depending on the size of the virtual machine disk and the capabilities of your storage hardware. When complete, the template is added to the **Templates** tab. You can now create new virtual machines based on the template.



Note

When a template is made, the virtual machine is copied so that both the existing virtual machine and its template are usable after template creation.

4.10.2.2. Explanation of Settings and Controls in the New Template Window

The following table details the settings for the **New Template** window.

Table 4.13. New Template and Edit Template Settings

Field	Description/Action
Name	The name of the template. This is the name by which the template is listed in the **Templates** tab in the Administration Portal and is accessed via the REST API. This text field has a 40-character limit and must be a unique name with any combination of uppercase and lowercase letters, numbers, hyphens, and underscores.
Description	A description of the template. This field is recommended but not mandatory.
Comment	A field for adding plain text, human-readable comments regarding the template.
Cluster	The cluster with which the template is associated. This is the same as the original virtual machines by default. You can select any cluster in the data center.

Field	Description/Action
CPU Profile	The CPU profile assigned to the template. CPU profiles define the maximum amount of processing capability a virtual machine can access on the host on which it runs, expressed as a percent of the total processing capability available to that host. CPU profiles are defined on the cluster level based on quality of service entries created for data centers.
Create as a Sub Template version	Specifies whether the template is created as a new version of an existing template. Select this check box to access the settings for configuring this option. - **Root Template**: The template under which the sub template is added. - **Sub Version Name**: The name of the template. This is the name by which the template is accessed when creating a new virtual machine based on the template.
Disks Allocation	**Alias** - An alias for the virtual machine disk used by the template. By default, the alias is set to the same value as that of the source virtual machine. **Virtual Size** - The current actual size of the virtual disk used by the template. This value cannot be edited, and is provided for reference only. **Target** - The storage domain on which the virtual disk used by the template is stored. By default, the storage domain is set to the same value as that of the source virtual machine. You can select any storage domain in the cluster.
Allow all users to access this Template	Specifies whether a template is public or private. A public template can be accessed by all users, whereas a private template can only be accessed by users with the **TemplateAdmin** or **SuperUser** roles.
Copy VM permissions	Copies explicit permissions that have been set on the source virtual machine to the template.

4.10.2.3. Editing a Template

Summary

Once a template has been created, its properties can be edited. Because a template is a copy of a virtual machine, the options available when editing a template are identical to those in the **Edit Virtual Machine** window.

Procedure 4.25. Editing a Template

1. Use the **Templates** resource tab, tree mode, or the search function to find and select the template in the results list.
2. Click **Edit** to open the **Edit Template** window.
3. Change the necessary properties and click **OK**.

Result

The properties of the template are updated. The **Edit Template** window does not close if a property field is invalid.

4.10.2.4. Deleting a Template

Summary

Delete a template from your Red Hat Enterprise Virtualization environment.

Warning

If you have used a template to create a virtual machine, make sure that you do not delete the template as the virtual machine needs it to continue running.

Procedure 4.26. Deleting a Template

1. Use the resource tabs, tree mode, or the search function to find and select the template in the results list.
2. Click **Remove** to open the **Remove Template(s)** window.
3. Click **OK** to remove the template.

Result

You have removed the template.

4.10.3. Sealing Templates in Preparation for Deployment

4.10.3.1. Sealing a Linux Virtual Machine for Deployment as a Template

There are two main methods for sealing a Linux virtual machine in preparation for using that virtual machine to create a template: manually, or using the **sys-unconfig** command. Sealing a Linux virtual machine manually requires you to create a file on the virtual machine that acts as a flag for initiating various configuration tasks the next time you start that virtual machine. The **sys-unconfig** command allows you to automate this process. However, both of these methods also require you to manually delete files on the virtual machine that are specific to that virtual machine or might cause conflicts amongst virtual machines created based on the template you will create based on that virtual machine. As such, both are valid methods for sealing a Linux virtual machine and will achieve the same result.

4.10.3.2. Sealing a Linux Virtual Machine Manually for Deployment as a Template

Summary

You must generalize (seal) a Linux virtual machine before creating a template based on that virtual machine.

Procedure 4.27. Sealing a Linux Virtual Machine

1. Log in to the virtual machine.
2. Flag the system for re-configuration by running the following command as root:

```
# touch /.unconfigured
```

3. Run the following command to remove ssh host keys:

```
# rm -rf /etc/ssh/ssh_host_*
```

4. Set **HOSTNAME=localhost.localdomain** in **/etc/sysconfig/network**
5. Run the following command to remove **/etc/udev/rules.d/70-***:

```
# rm -rf /etc/udev/rules.d/70-*
```

6. Remove the **HWADDR** line and **UUID** line from **/etc/sysconfig/network-scripts/ifcfg-eth***.
7. Optionally, delete all the logs from **/var/log** and build logs from **/root**.
8. Run the following command to shut down the virtual machine:

```
# poweroff
```

Result

The virtual machine is sealed and can be made into a template. You can deploy Linux virtual machines from this template without experiencing configuration file conflicts.

4.10.3.3. Sealing a Linux Virtual Machine for Deployment as a Template using sys-unconfig

Summary

You must generalize (seal) a Linux virtual machine before creating a template based on that virtual machine.

Procedure 4.28. Sealing a Linux Virtual Machine using sys-unconfig

1. Log in to the virtual machine.
2. Run the following command to remove ssh host keys:

```
# rm -rf /etc/ssh/ssh_host_*
```

3. Set **HOSTNAME=localhost.localdomain** in **/etc/sysconfig/network**.
4. Remove the **HWADDR** line and **UUID** line from **/etc/sysconfig/network-scripts/ifcfg-eth***.

5. Optionally, delete all the logs from **/var/log** and build logs from **/root**.
6. Run the following command:

```
# sys-unconfig
```

Result

The virtual machine shuts down; it is now sealed and can be made into a template. You can deploy Linux virtual machines from this template without experiencing configuration file conflicts.

4.10.3.4. Sealing a Windows Template

4.10.3.4.1. Considerations when Sealing a Windows Template with Sysprep

A template created for Windows virtual machines must be generalized (sealed) before being used to deploy virtual machines. This ensures that machine-specific settings are not reproduced in the template.

The **Sysprep** tool is used to seal Windows templates before use.

Important

Do not reboot the virtual machine during this process.

Before starting the **Sysprep** process, verify that the following settings are configured:

- The Windows **Sysprep** parameters have been correctly defined.

  If not, click **Edit** and enter the required information in the **Operating System** and **Domain** fields.

- The correct product key has been defined in an override file under **/etc/ovirt-engine/osinfo.conf.d/10-productkeys.properties** on the Manager.

  If not, copy the default values for your Windows operating system from **/etc/ovirt-engine/osinfo.conf.d/00-defaults.properties** into the override file, and input your values in the **productKey.value** and **sysprepPath.value** fields.

Example 4.1. Windows 7 Default Configuration Values

```
# Windows7(11, OsType.Windows, false),false
os.windows_7.id.value = 11
os.windows_7.name.value = Windows 7
os.windows_7.derivedFrom.value = windows_xp
os.windows_7.sysprepPath.value =
${ENGINE_USR}/conf/sysprep/sysprep.w7
os.windows_7.productKey.value =
os.windows_7.devices.audio.value = ich6
os.windows_7.devices.diskInterfaces.value.3.3 = IDE, VirtIO_SCSI,
VirtIO
os.windows_7.devices.diskInterfaces.value.3.4 = IDE, VirtIO_SCSI,
```

```
VirtIO
os.windows_7.devices.diskInterfaces.value.3.5 = IDE, VirtIO_SCSI,
VirtIO
os.windows_7.isTimezoneTypeInteger.value = false
```

4.10.3.4.2. Sealing a Windows XP Template

Summary

Seal a Windows XP template using the **Sysprep** tool before using the template to deploy virtual machines.

Note

You can also use the procedure above to seal a Windows 2003 template. The Windows 2003 **Sysprep** tool is available at http://www.microsoft.com/download/en/details.aspx?id=14830.

Procedure 4.29. Sealing a Windows XP Template

1. Download **sysprep** to the virtual machine to be used as a template.

   The Windows XP **Sysprep** tool is available at http://www.microsoft.com/download/en/details.aspx?id=11282

2. Create a new directory: **c:\sysprep**.
3. Open the **deploy.cab** file and add its contents to **c:\sysprep**.
4. Execute **sysprep.exe** from within the folder and click **OK** on the welcome message to display the Sysprep tool.
5. Select the following check boxes:
   - **Don't reset grace period for activation**
   - **Use Mini-Setup**
6. Ensure that the shutdown mode is set to **Shut down** and click **Reseal**.
7. Acknowledge the pop-up window to complete the sealing process; the virtual machine shuts down automatically upon completion.

Result

The Windows XP template is sealed and ready for deploying virtual machines.

4.10.3.4.3. Sealing a Windows 7 or Windows 2008 Template

Summary

Seal a Windows 7 or Windows 2008 template before using the template to deploy virtual machines.

Procedure 4.30. Sealing a Windows 7 or Windows 2008 Template

1. In the virtual machine to be used as a template, open a command line terminal and type **regedit**.
2. The **Registry Editor** window opens. On the left pane, expand **HKEY_LOCAL_MACHINE** → **SYSTEM** → **SETUP**.
3. On the main window, right-click to add a new string value using **New** → **String Value**.
4. Right-click on the file and select **Modify** to open the **Edit String** window.
5. Enter the following information in the provided fields:
   - Value name: **UnattendFile**
   - Value data: **a:\sysprep.inf**
6. Launch **Sysprep** from **C:\Windows\System32\sysprep\sysprep.exe**.
7. Enter the following information into the **Sysprep** tool:
   - Under **System Cleanup Action**, select **Enter System Out-of-Box-Experience (OOBE)**.
   - Select the **Generalize** check box if you need to change the computer's system identification number (SID).
   - Under **Shutdown Options**, select **Shutdown**.

   Click **OK** to complete the sealing process; the virtual machine shuts down automatically upon completion.

Result

The Windows 7 or Windows 2008 template is sealed and ready for deploying virtual machines.

4.10.3.5. Using Cloud-Init to Automate the Configuration of Virtual Machines

4.10.3.5.1. Cloud-Init Overview

Cloud-Init is a tool for automating the initial setup of virtual machines such as configuring the host name, network interfaces, and authorized keys. It can be used when provisioning virtual machines that have been deployed based on a template to avoid conflicts on the network.

To use this tool, the *cloud-init* package must first be installed on the virtual machine. Once installed, the Cloud-Init service starts during the boot process to search for instructions on what to configure. You can then use options in the **Run Once** window to provide these instructions one time only, or options in the **New Virtual Machine**, **Edit Virtual Machine** and **Edit Template** windows to provide these instructions every time the virtual machine starts.

4.10.3.5.2. Cloud-Init Use Case Scenarios

Cloud-Init can be used to automate the configuration of virtual machines in a variety of scenarios. Several common scenarios are as follows:

Virtual Machines Created Based on Templates

You can use the Cloud-Init options in the **Initial Run** section of the **Run Once** window to initialize a virtual machine that was created based on a template. This allows you to customize the virtual machine the first time that virtual machine is started.

Virtual Machine Templates

You can use the **Use Cloud-Init/Sysprep** options in the **Initial Run** tab of the **New Template** and **Edit Template** windows to specify options for customizing virtual machines created based on that template.

Virtual Machine Pools

You can use the **Use Cloud-Init/Sysprep** options in the **Initial Run** tab of the **New Pool** window to specify options for customizing virtual machines taken from that virtual machine pool. This allows you to specify a set of standard settings that will be applied every time a virtual machine is taken from that virtual machine pool. You can inherit or override the options specified for the template on which the virtual machine is based, or specify options for the virtual machine pool itself.

4.10.3.5.3. Installing Cloud-Init

Summary

Install Cloud-Init on a virtual machine.

Procedure 4.31. Installing Cloud-Init

1. Log on to the virtual machine.
2. Enable the Red Hat Common channel.

```
# subscription-manager repos --enable=rhel-6-server-rh-common-rpms
```

3. Install the *cloud-init* package and dependencies:

```
# yum install cloud-init
```

Result

You have installed the *cloud-init* package and dependencies.

4.10.3.5.4. Using Cloud-Init to Initialize a Virtual Machine

Summary

Use Cloud-Init to automate the initial configuration of a Linux virtual machine that has been provisioned based on a template.

Procedure 4.32. Using Cloud-Init to Initialize a Virtual Machine

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click **Run Once** to open the **Run Virtual Machine(s)** window.
3. Expand the **Initial Run** section and select the **Cloud-Init** check box.
4. Enter a host name in the **VM Hostname** text field.
5. Select the **Configure Time Zone** check box and select a time zone from the **Time Zone** drop-down menu.

6. Select the **Use already configured password** check box to use the existing credentials, or clear that check box and enter a root password in the **Password** and **Verify Password** text fields to specify a new root password.
7. Enter any SSH keys to be added to the authorized hosts file on the virtual machine in the **SSH Authorized Keys** text area.
8. Select the **Regenerate SSH Keys** check box to regenerate SSH keys for the virtual machine.
9. Enter any DNS servers in the **DNS Servers** text field.
10. Enter any DNS search domains in the **DNS Search Domains** text field.
11. Select the **Network** check box and use the **+** and **-** buttons to add or remove network interfaces to or from the virtual machine.
12. Enter any custom scripts in the **Custom Script** text area.
13. Click **OK**.

Important

Cloud-Init is only supported on cluster compatibility version 3.3 and higher.

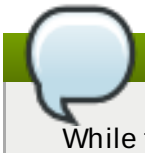
Result

The virtual machine boots and the specified settings are applied.

4.10.3.5.5. Using Cloud-Init to Prepare a Template

Summary

Use Cloud-Init to specify a set of standard settings to be included in a template.



Note

While the following procedure outlines how to use Cloud-Init when preparing a template, the same settings are also available in the **New Virtual Machine** and **Edit Template** windows.

Procedure 4.33. Using Cloud-Init to Prepare a Template

1. Click the **Virtual Machines** tab and select a virtual machine.
2. Click **Edit** to open the **Edit Virtual Machine** window.
3. Click the **Initial Run** tab and select the **Use Cloud-Init/Sysprep** check box.
4. Enter a host name in the **VM Hostname** text field.
5. Select the **Configure Time Zone** check box and select a time zone from the **Time Zone** drop-down menu.

6. Expand the **Authentication** section and select the **Use already configured password** check box to user the existing credentials, or clear that check box and enter a root password in the **Password** and **Verify Password** text fields to specify a new root password.
7. Enter any SSH keys to be added to the authorized hosts file on the virtual machine in the **SSH Authorized Keys** text area.
8. Select the **Regenerate SSH Keys** check box to regenerate SSH keys for the virtual machine.
9. Expand the **Networks** section and enter any DNS servers in the **DNS Servers** text field.
10. Enter any DNS search domains in the **DNS Search Domains** text field.
11. Select the **Network** check box and use the **+** and **-** buttons to add or remove network interfaces to or from the virtual machine.
12. Expand the **Custom Script** section and enter any custom scripts in the **Custom Script** text area.
13. Click **Ok**.

Important

Cloud-Init is only supported on cluster compatibility version 3.3 and higher.

Result

The virtual machine boots and the specified settings are applied.

4.10.4. Templates and Permissions

4.10.4.1. Managing System Permissions for a Template

As the **SuperUser**, the system administrator manages all aspects of the Administration Portal. More specific administrative roles can be assigned to other users. These restricted administrator roles are useful for granting a user administrative privileges that limit them to a specific resource. For example, a **DataCenterAdmin** role has administrator privileges only for the assigned data center with the exception of the storage for that data center, and a **ClusterAdmin** has administrator privileges only for the assigned cluster.

A template administrator is a system administration role for templates in a data center. This role can be applied to specific virtual machines, to a data center, or to the whole virtualized environment; this is useful to allow different users to manage certain virtual resources.

The template administrator role permits the following actions:

- Create, edit, export, and remove associated templates.
- Import and export templates.

Note

You can only assign roles and permissions to existing users.

4.10.4.2. Template Administrator Roles Explained

Template Administrator Permission Roles

The table below describes the administrator roles and privileges applicable to template administration.

Table 4.14. Red Hat Enterprise Virtualization System Administrator Roles

Role	Privileges	Notes
TemplateAdmin	Can perform all operations on templates.	Has privileges to create, delete and configure a template's storage domain and network details, and to move templates between domains.
NetworkAdmin	Network Administrator	Can configure and manage networks attached to templates.

4.10.4.3. Template User Roles Explained

Template User Permission Roles

The table below describes the user roles and privileges applicable to using and administrating templates in the User Portal.

Table 4.15. Red Hat Enterprise Virtualization Template User Roles

Role	Privileges	Notes
TemplateCreator	Can create, edit, manage and remove virtual machine templates within assigned resources.	The **TemplateCreator** role is not applied to a specific template; apply this role to a user for the whole environment with the **Configure** window. Alternatively apply this role for specific data centers, clusters, or storage domains.
TemplateOwner	Can edit and delete the template, assign and manage user permissions for the template.	The **TemplateOwner** role is automatically assigned to the user who creates a template. Other users who do not have **TemplateOwner** permissions on a template cannot view or use the template.
UserTemplateBasedVm	Can use the template to create virtual machines.	Cannot edit template properties.

Role	Privileges	Notes
NetworkUser	Logical network and network interface user for templates.	If the **Allow all users to use this Network** option was selected when a logical network is created, **NetworkUser** permissions are assigned to all users for the logical network. Users can then attach or detach template network interfaces to or from the logical network.

4.11. Resources

4.11.1. Monitoring Resources

Before making configuration changes to virtual machines in the User Portal, it is recommended that you take an inventory of the resources available. This is to ensure the resources are sufficient for peak performance and to avoid overloading the hosts running the virtual machines.

The **Resources** tab in the navigation pane shows a cumulative view of all the resources available in the User Portal, and the performance and statistics of each virtual machine.

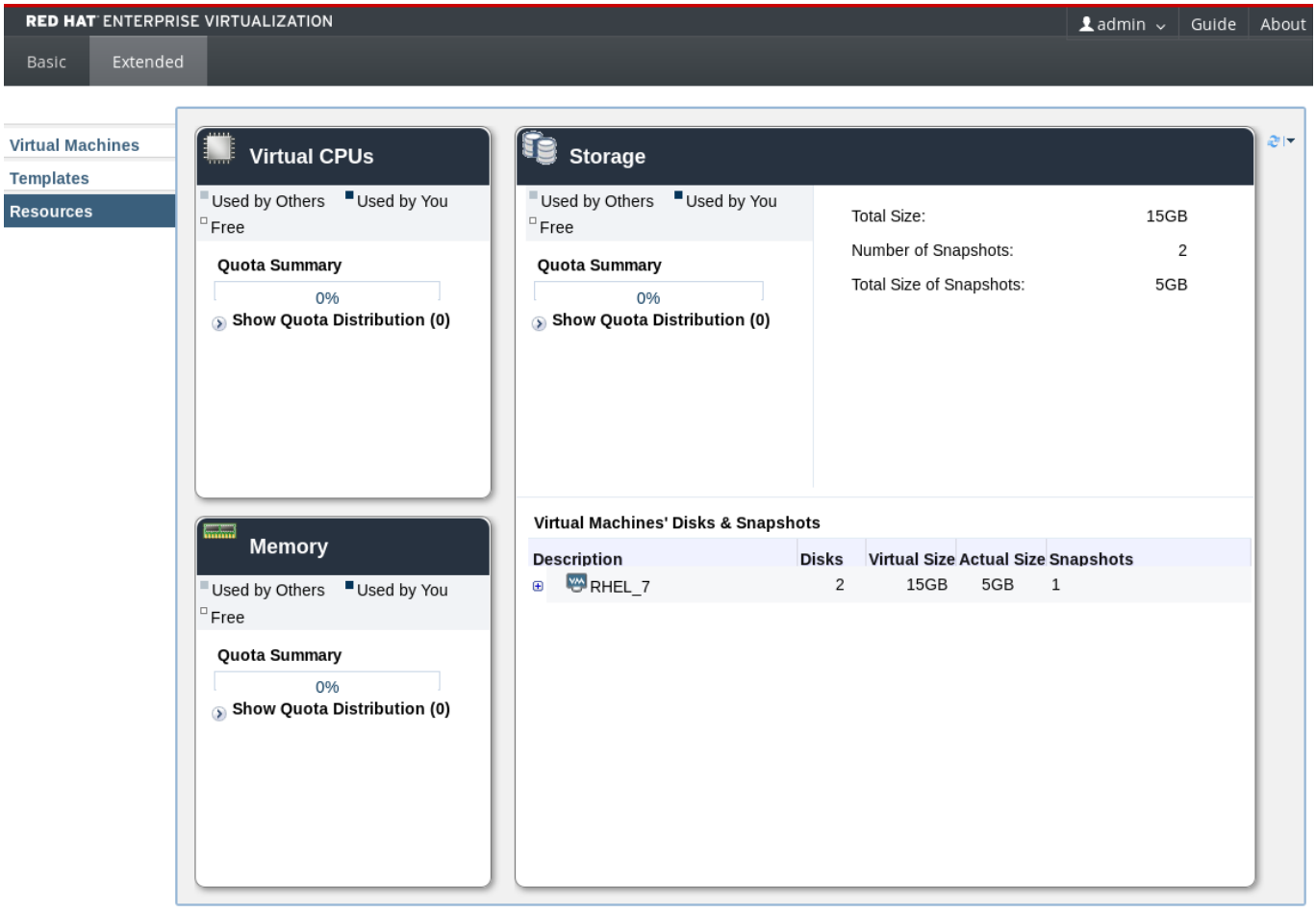


Figure 4.12. Resources tab

- **Virtual CPUs**: This box displays the number of your machines' virtual CPUs in use, and the

consumption of CPU quota used by you and others.

- **Memory**: This box displays the consumption of memory quota used by you and others, and available memory as defined by the quota.
- **Storage**: This box displays the consumption of storage quota by you and others, the total size of all your virtual disks, and the number and total size of your virtual machines' snapshots. It also displays a breakdown of storage details for each virtual machine. Click the **+** button next to the virtual machine name to display all the virtual disks attached to the virtual machine.

4.11.2. Quota - A User's Introduction

When you create a virtual machine, the virtual machine consumes CPU and storage resources from its data center. Quota compares the amount of virtual resources consumed by the creation of the virtual machine to the storage allowance and the run-time allowance set by the system administrator.

If you do not have enough of either kind of allowance, you are not allowed to create the virtual machine. Avoid exceeding your quota limit by using the Resources tab to monitor your CPU and storage consumption.

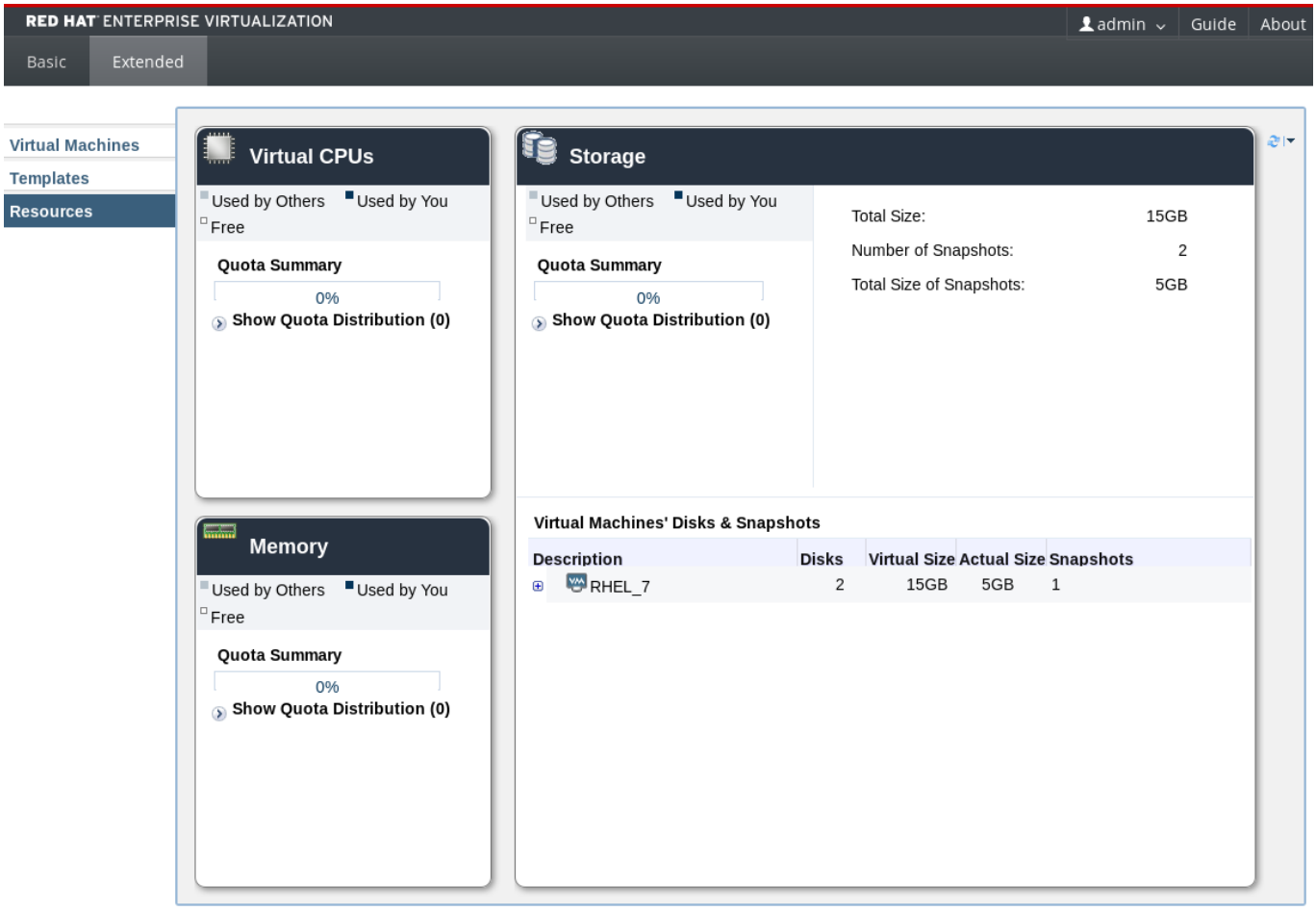


Figure 4.13. Resources tab

4.11.3. What to Do When You Exceed Your Quota

Red Hat Enterprise Virtualization provides a resource-limitation tool called *quota*, which allows system administrators to limit the amount of CPU and storage each user can consume. Quota compares the amount of virtual resources consumed when you use the virtual machine to the storage allowance and the run-time allowance set by the system administrator.

When you exceed your quota, a pop-up window informs you that you have exceeded your quota, and you will no longer have access to virtual resources. For example, this can happen if you have too many concurrently running virtual machines in your environment.

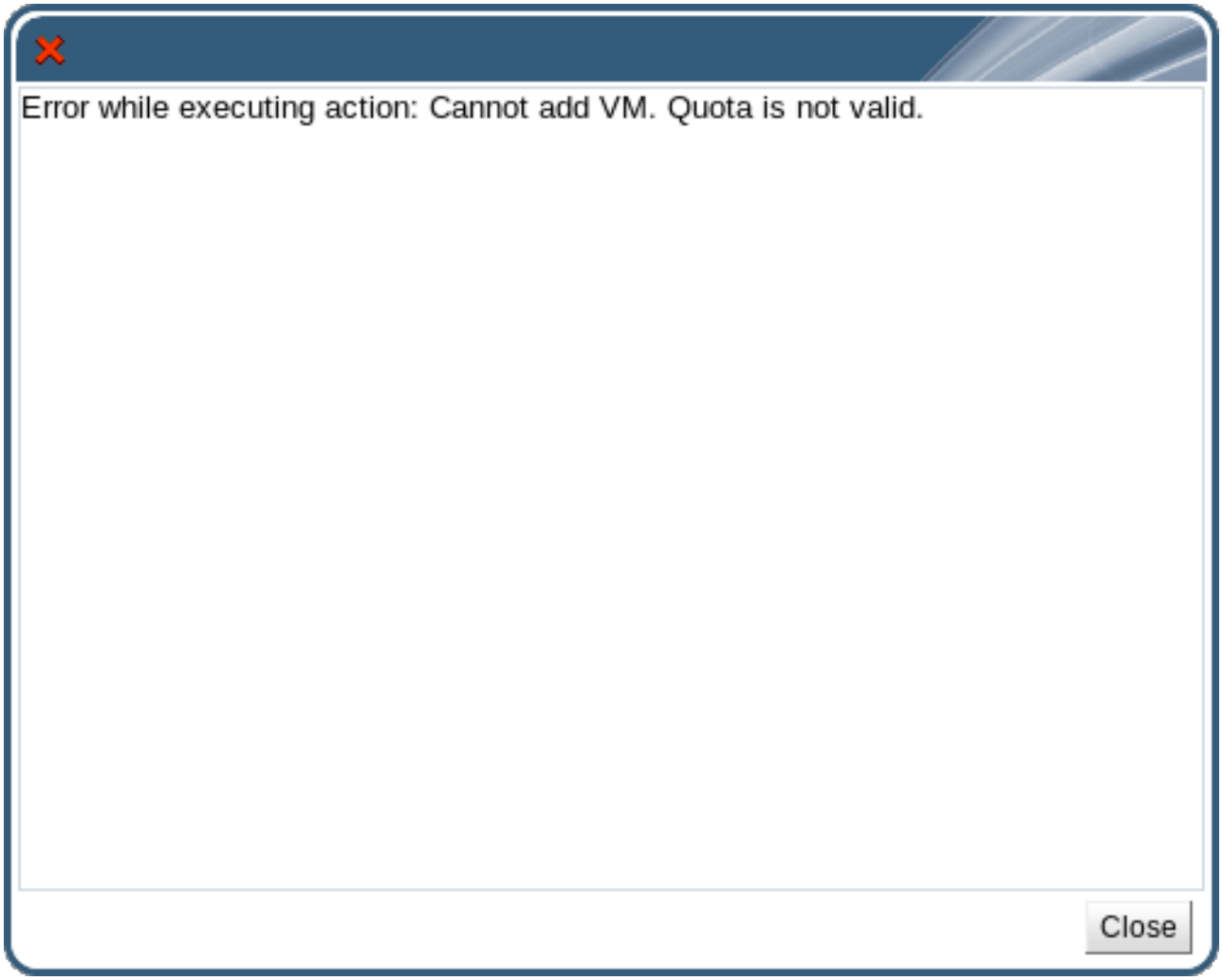


Figure 4.14. Quota exceeded error message

To regain access to your virtual machines, do one of the following:

- Shut down the virtual machines that you do not need. This will bring your resource consumption down to a level at which it is not in excess of the quota, and you will be able to run virtual machines again.
- If you cannot shut down any existing virtual machines, contact your system administrator to extend your quota allowance or remove any unused virtual machines.

4.12. Virtual Machines and Permissions

4.12.1. Managing System Permissions for a Virtual Machine

As the **SuperUser**, the system administrator manages all aspects of the Administration Portal. More specific administrative roles can be assigned to other users. These restricted administrator roles are useful for granting a user administrative privileges that limit them to a specific resource. For example, a **DataCenterAdmin** role has administrator privileges only for the assigned data center with the

exception of the storage for that data center, and a **ClusterAdmin** has administrator privileges only for the assigned cluster.

A **UserVmManager** is a system administration role for virtual machines in a data center. This role can be applied to specific virtual machines, to a data center, or to the whole virtualized environment; this is useful to allow different users to manage certain virtual resources.

The user virtual machine administrator role permits the following actions:

- Create, edit, and remove virtual machines.
- Run, suspend, shutdown, and stop virtual machines.

Note

You can only assign roles and permissions to existing users.

Many end users are concerned solely with the virtual machine resources of the virtualized environment. As a result, Red Hat Enterprise Virtualization provides several user roles which enable the user to manage virtual machines specifically, but not other resources in the data center.

4.12.2. Virtual Machines Administrator Roles Explained

Virtual Machine Administrator Permission Roles

The table below describes the administrator roles and privileges applicable to virtual machine administration.

Table 4.16. Red Hat Enterprise Virtualization System Administrator Roles

Role	Privileges	Notes
DataCenterAdmin	Data Center Administrator	Possesses administrative permissions for all objects underneath a specific data center except for storage.
ClusterAdmin	Cluster Administrator	Possesses administrative permissions for all objects underneath a specific cluster.
NetworkAdmin	Network Administrator	Possesses administrative permissions for all operations on a specific logical network. Can configure and manage networks attached to virtual machines. To configure port mirroring on a virtual machine network, apply the **NetworkAdmin** role on the network and the **UserVmManager** role on the virtual machine.

4.12.3. Virtual Machine User Roles Explained

Virtual Machine User Permission Roles

The table below describes the user roles and privileges applicable to virtual machine users. These roles allow access to the User Portal for managing and accessing virtual machines, but they do not confer any permissions for the Administration Portal.

Table 4.17. Red Hat Enterprise Virtualization System User Roles

Role	Privileges	Notes
UserRole	Can access and use virtual machines and pools.	Can log in to the User Portal and use virtual machines and pools.
PowerUserRole	Can create and manage virtual machines and templates.	Apply this role to a user for the whole environment with the **Configure** window, or for specific data centers or clusters. For example, if a PowerUserRole is applied on a data center level, the PowerUser can create virtual machines and templates in the data center. Having a **PowerUserRole** is equivalent to having the **VmCreator**, **DiskCreator**, and **TemplateCreator** roles.
UserVmManager	System administrator of a virtual machine.	Can manage virtual machines, create and use snapshots, and migrate virtual machines. A user who creates a virtual machine in the User Portal is automatically assigned the UserVmManager role on the machine.
UserTemplateBasedVm	Limited privileges to only use Templates.	Level of privilege to create a virtual machine by means of a template.
VmCreator	Can create virtual machines in the User Portal.	This role is not applied to a specific virtual machine; apply this role to a user for the whole environment with the **Configure** window. When applying this role to a cluster, you must also apply the **DiskCreator** role on an entire data center, or on specific storage domains.

Role	Privileges	Notes
NetworkUser	Logical network and network interface user for virtual machines.	If the **Allow all users to use this Network** option was selected when a logical network is created, **NetworkUser** permissions are assigned to all users for the logical network. Users can then attach or detach virtual machine network interfaces to or from the logical network.

4.12.4. Assigning Virtual Machines to Users

If you are creating virtual machines for users other than yourself, you have to assign roles to the users before they can use the virtual machines. Note that permissions can only be assigned to existing users. See the *Red Hat Enterprise Virtualization Installation Guide* for details on creating user accounts.

The Red Hat Enterprise Virtualization User Portal supports three default roles: User, PowerUser and UserVmManager. However, customized roles can be configured via the Red Hat Enterprise Virtualization Manager Administration Portal. The default roles are described below.

- A **User** can connect to and use virtual machines. This role is suitable for desktop end users performing day-to-day tasks.
- A **PowerUser** can create virtual machines and view virtual resources. This role is suitable if you are an administrator or manager who needs to provide virtual resources for your employees.
- A **UserVmManager** can edit and remove virtual machines, assign user permissions, use snapshots and use templates. It is suitable if you need to make configuration changes to your virtual environment.

When you create a virtual machine, you automatically inherit **UserVmManager** privileges. This enables you to make changes to the virtual machine and assign permissions to the users you manage, or users who are in your Identity Management (IdM) or RHDS group.

See *Red Hat Enterprise Virtualization Installation Guide* for more information on directory services support in Red Hat Enterprise Virtualization.

Summary

This procedure explains how to add permissions to users.

Procedure 4.34. Assigning Permissions to Users

1. Click the **Virtual Machines** tab and select a virtual machine.
2. On the details pane, select the **Permissions** tab.
3. Click **New**. The **Add Permission to User** dialog displays. Enter a Name, or User Name, or part thereof in the **Search** text box, and click **Go**. A list of possible matches display in the results list.
4. Select the check box of the user to be assigned the permissions. Scroll through the **Role to Assign** list and select **UserRole**. Click **OK**.

5. The user's name and role display in the list of users permitted to access this virtual machine.

Result

You have added permissions to a user.

Note

If a user is assigned permissions to only one virtual machine, single sign-on (SSO) can be configured for the virtual machine. With single sign-on enabled, when a user logs in to the User Portal, and then connects to a virtual machine through, for example, a SPICE console, users are automatically logged in to the virtual machine and do not need to type in the username and password again. Single sign-on can be enabled or disabled via the User Portal on a per virtual machine basis. See the *User Guide* for more information on how to enable and disable single sign-on for virtual machines.

4.12.5. Removing Access to Virtual Machines from Users

Summary

This procedure explains how to remove user permissions.

Procedure 4.35. Removing Access to Virtual Machines from Users

1. Click the **Virtual Machines** tab and select a virtual machine.
2. On the details pane, select the **Permissions** tab.
3. Click **Remove**. A warning message displays, asking you to confirm removal of the selected permissions.
4. To proceed, click **OK**. To abort, click **Cancel**.

Result

You have now removed permissions from a user.

Part III. Advanced Usage

1. Introduction to Using Virtual Machines - Advanced

This chapter describes how to configure advanced operations on virtual machines. It includes:

- Configuration of protocol options
- Use of USB devices with virtual machines
- Support for multiple monitors

Chapter 5. Guest Drivers and Agents

5.1. Installing the Guest Agents and Drivers

The Red Hat Enterprise Virtualization guest agents and drivers are a set of components that you can install on Red Hat Enterprise Linux and Windows virtual machines in your Red Hat Enterprise Virtualization environment to provide additional information about and functionality for those virtual machines. Key features include the ability to monitor resource usage, gracefully shut down or reboot virtual machines from the User Portal and Administration Portal. To access this functionality, you must install the Red Hat Enterprise Virtualization guest agents and drivers on each virtual machine on which this functionality is to be available.

5.2. Installing the Guest Agents and Drivers on Red Hat Enterprise Linux

Summary

The Red Hat Enterprise Virtualization guest agents and drivers are installed on Red Hat Enterprise Linux virtual machines using the **rhevm-guest-agent** package provided by the Red Hat Enterprise Virtualization Agent channel.

Procedure 5.1. Installing the Guest Agents and Drivers on Red Hat Enterprise Linux

1. Log in to the Red Hat Enterprise Linux virtual machine.
2. Enable the Red Hat Enterprise Virtualization Agent channel:
   - For Red Hat Enterprise Linux 6

     ```
     # subscription-manager repos --enable=rhel-6-server-rhev-agent-rpms
     ```

   - For Red Hat Enterprise Linux 7

     ```
     # subscription-manager repos --enable=rhel-7-server-rh-common-rpms
     ```

3. Install the *rhevm-guest-agent-common* package and dependencies:

   ```
   # yum install rhevm-guest-agent-common
   ```

Result

You have installed the guest agent, which now passes usage information to the Red Hat Enterprise Virtualization Manager. The Red Hat Enterprise Virtualization agent runs as a service called **ovirt-guest-agent** that you can configure via the **ovirt-guest-agent.conf** configuration file in the **/etc/** directory.

5.3. Installing the Guest Agents and Drivers on Windows

Summary

The Red Hat Enterprise Virtualization guest agents and drivers are installed on Windows virtual machines using the **rhev-tools-setup.iso** ISO file, which is provided by the *rhev-guest-tools-iso* package installed as a dependency to the Red Hat Enterprise Virtualization Manager. This ISO file is located in **/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso** on the system on which the Red Hat Enterprise Virtualization Manager is installed.

Note

The **rhev-tools-setup.iso** ISO file is automatically copied to the default ISO storage domain, if any, when you run **engine-setup**, or must be manually uploaded to an ISO storage domain.

Note

Updated versions of the **rhev-tools-setup.iso** ISO file must be manually attached to running Windows virtual machines to install updated versions of the tools and drivers. If the APT service is enabled on virtual machines, the updated ISO files will be automatically attached.

Note

If you install the guest agents and drivers from the command line or as part of a deployment tool such as Windows Deployment Services, you can append the options **ISSILENTMODE** and **ISNOREBOOT** to **RHEV-toolsSetup.exe** to silently install the guest agents and drivers and prevent the machine on which they have been installed from rebooting immediately after installation. The machine can then be rebooted later once the deployment process is complete.

```
D:\RHEV-toolsSetup.exe ISSILENTMODE ISNOREBOOT
```

Procedure 5.2. Installing the Guest Agents and Drivers on Windows

1. Log in to the virtual machine.
2. Select the CD Drive containing the **rhev-tools-setup.iso** file.
3. Double-click **RHEV-toolsSetup**.
4. Click **Next** at the welcome screen.
5. Click **Yes** in the **User Account Control** window.
6. Follow the prompts on the **RHEV-Tools InstallShield Wizard** window. Ensure all check boxes in the list of components are selected.

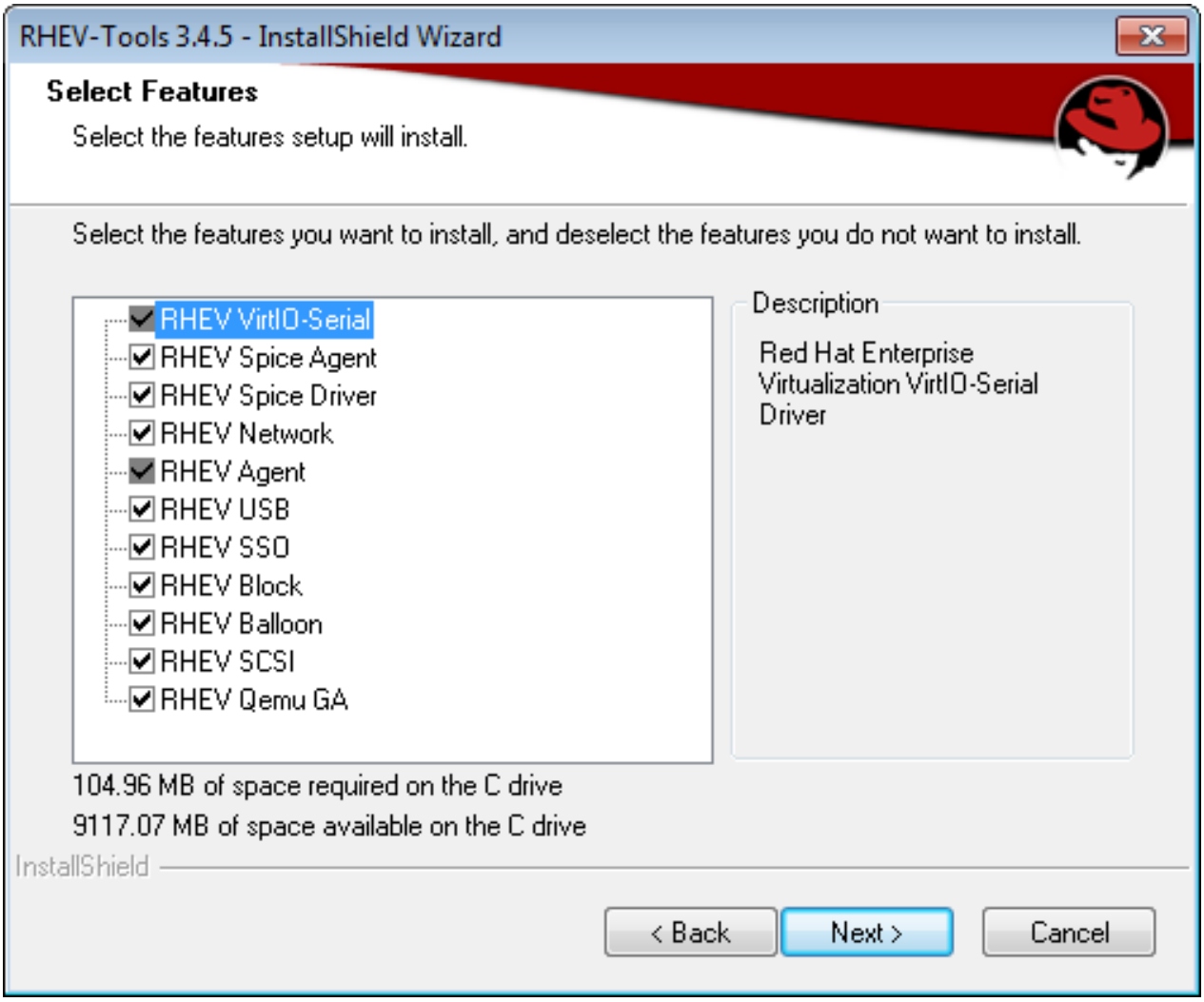


Figure 5.1. Selecting All Components of Red Hat Enterprise Virtualization Tools for Installation

7. Once installation is complete, select **`Yes, I want to restart my computer now`** and click **`Finish`** to apply the changes.

Result

You have installed the guest agents and drivers, which now pass usage information to the Red Hat Enterprise Virtualization Manager and allow you to access USB devices, single sign-on into virual machines and other functionality. The Red Hat Enterprise Virtualization guest agent runs as a service called **`RHEV Agent`** that you can configure using the **`rhev-agent`** configuration file located in **`C:\Program Files\Redhat\RHEV\Drivers\Agent`**.

5.4. Automating Guest Additions on Windows Guests with Red Hat Enterprise Virtualization Application Provisioning Tool(APT)

Summary

Red Hat Enterprise Virtualization Application Provisioning Tool (APT) is a Windows service that can be installed on Windows virtual machines and templates. When the APT service is installed and running on a virtual machine, attached ISO files are automatically scanned. When the service recognizes a valid Red Hat Enterprise Virtualization guest tools ISO, and no other guest tools are

installed, the APT service installs the guest tools. If guest tools are already installed, and the ISO image contains newer versions of the tools, the service performs an automatic upgrade. This procedure assumes you have attached the **rhev-tools-setup.iso** ISO file to the virtual machine.

Procedure 5.3. Installing the APT Service on Windows

1. Log in to the virtual machine.
2. Select the CD Drive containing the **rhev-tools-setup.iso** file.
3. Double-click **RHEV-Application Provisioning Tool**.
4. Click **Yes** in the **User Account Control** window.
5. Once installation is complete, ensure the **Start RHEV-apt Service** check box is selected in the **RHEV-Application Provisioning Tool InstallShield Wizard** window, and click **Finish** to apply the changes.

Result

You have installed and started the APT service.

Once the APT service has successfully installed or upgraded the guest tools on a virtual machine, the virtual machine is automatically rebooted; this happens without confirmation from the user logged in to the machine. The APT Service will also perform these operations when a virtual machine created from a template that has the APT Service already installed is booted for the first time.

Note

The **RHEV-apt** service can be stopped immediately after install by clearing the **Start RHEV-apt Service** check box. You can stop, start, or restart the service at any time using the **Services** window.

5.5. Red Hat Enterprise Virtualization Guest Drivers and Guest Agents

Red Hat Enterprise Virtualization provides customized drivers and guest tools to use with Windows and Red Hat Enterprise Linux guests. The drivers allow guests to use enhanced virtual devices that perform better than emulated devices; the guest agents facilitate communication between the guest and the Red Hat Enterprise Virtualization Manager.

Table 5.1. Red Hat Enterprise Virtualization Guest Drivers

Driver	Description	Works on
virtio-net	Paravirtualized network driver provides enhanced performance over emulated devices like rtl.	Server and Desktop.

Driver	Description	Works on
virtio-block	Paravirtualized HDD driver offers increased I/O performance over emulated devices like IDE by optimizing the coordination and communication between the guest and the hypervisor. The driver complements the software implementation of the virtio-device used by the host to play the role of a hardware device.	Server and Desktop.
virtio-scsi	Paravirtualized iSCSI HDD driver offers similar functionality to the virtio-block device, with some additional enhancements. In particular, this driver supports adding hundreds of devices, and names devices using the standard SCSI device naming scheme.	Server and Desktop.
virtio-serial	Virtio-serial provides support for multiple serial ports. The improved performance is used for fast communication between the guest and the host that avoids network complications. This fast communication is required for the guest agents and for other features such as clipboard copy-paste between the guest and the host and logging.	Server and Desktop.
virtio-balloon	Virtio-balloon is used to control the amount of memory a guest actually accesses. It offers improved memory over-commitment. The balloon drivers are installed for future compatibility but not used by default in Red Hat Enterprise Virtualization 3.1 or higher.	Server and Desktop.
qxl	A paravirtualized display driver reduces CPU usage on the host and provides better performance through reduced network bandwidth on most workloads.	Server and Desktop.

Table 5.2. Red Hat Enterprise Virtualization Guest Agents and Tools

Guest agent/tool	Description	Works on
rhevm-guest-agent-common	Allows the Red Hat Enterprise Virtualization Manager to receive guest internal events and information such as IP address and installed applications. Also allows the Manager to execute specific commands, such as shut down or reboot, on a guest. On Red Hat Enterprise Linux 6 and higher guests, the rhevm-guest-agent-common installs **tuned** on your virtual machine and configures it to use an optimized, virtualized-guest profile.	Server and Desktop.
spice-agent	The SPICE agent supports multiple monitors and is responsible for client-mouse-mode support to provide a better user experience and improved responsiveness than the QEMU emulation. Cursor capture is not needed in client-mouse-mode. The SPICE agent reduces bandwidth usage when used over a wide area network by reducing the display level, including color depth, disabling wallpaper, font smoothing, and animation. The SPICE agent enables clipboard support allowing cut and paste operations for both text and images between client and guest, and automatic guest display setting according to client-side settings. On Windows guests, the SPICE agent consists of vdservice and vdagent.	Server and Desktop.
rhev-sso	An agent that enables users to automatically log in to their virtual machines based on the credentials used to access the Red Hat Enterprise Virtualization Manager.	Desktop.

Guest agent/tool	Description	Works on
rhev-usb	A component that contains drivers and services for Legacy USB support (version 3.0 and earlier) on guests. It is needed for accessing a USB device that is plugged into the client machine. **RHEV-USB Client** is needed on the client side.	Desktop.

Chapter 6. Configuring Console Options

6.1. Console Options

6.1.1. Introduction to Connection Protocols

Connection protocols are the underlying technology used to provide graphical consoles for virtual machines and allow users to work with virtual machines in a similar way as they would with physical machines. Red Hat Enterprise Virtualization currently supports the following connection protocols:

SPICE

Simple Protocol for Independent Computing Environments (SPICE) is the recommended connection protocol for both Linux virtual machines and Windows virtual machines. SPICE is installed and executed on the client that connects to the virtual machine.

VNC

Virtual Network Computing (VNC) can be used to open consoles to both Linux virtual machines and Windows virtual machines. To open a console to a virtual machine using VNC, you must use Remote Viewer or a VNC client.

RDP

Remote Desktop Protocol (RDP) can only be used to open consoles to Windows virtual machines, and is only available when you access a virtual machines from a Windows machine on which Remote Desktop has been installed. Moreover, before you can connect to a Windows virtual machine using RDP, you must set up remote sharing on the virtual machine and configure the firewall to allow remote desktop connections.

Note

SPICE is not currently supported on virtual machines running Windows 8. If a Windows 8 virtual machine is configured to use the SPICE protocol, it will detect the absence of the required SPICE drivers and automatically fall back to using RDP.

6.1.2. Accessing Console Options

In the User Portal, you can configure several options for opening graphical consoles for virtual machines, such as the method of invocation and whether to enable or disable USB redirection.

Procedure 6.1. Accessing Console Options

1. Select a running virtual machine.
2. Click the edit console options button to open the **Console Options** window.

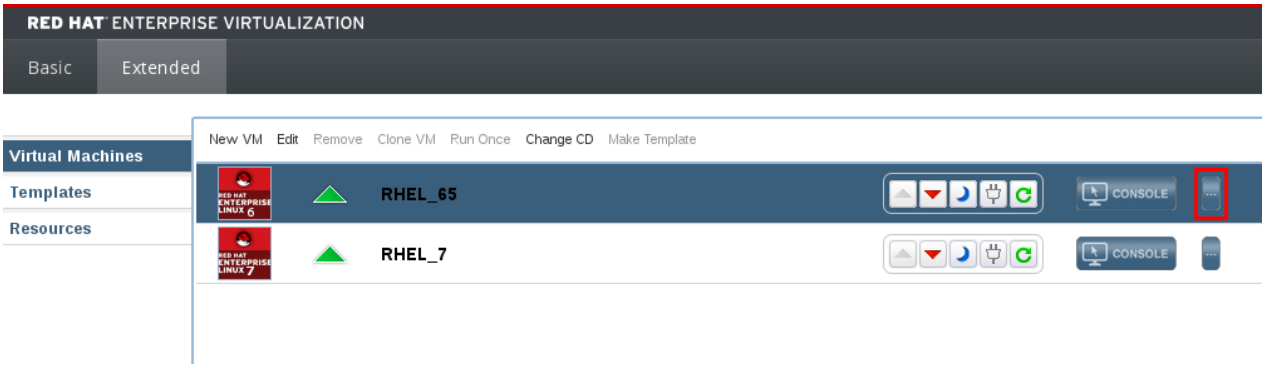
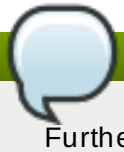


Figure 6.1. The edit console options button



Note

Further options specific to each of the connection protocols, such as the keyboard layout when using the VNC connection protocol, can be configured in the **Console** tab of the **Edit Virtual Machine** window.

6.1.3. SPICE Console Options

When the SPICE connection protocol is selected, the following options are available in the **Console Options** window.

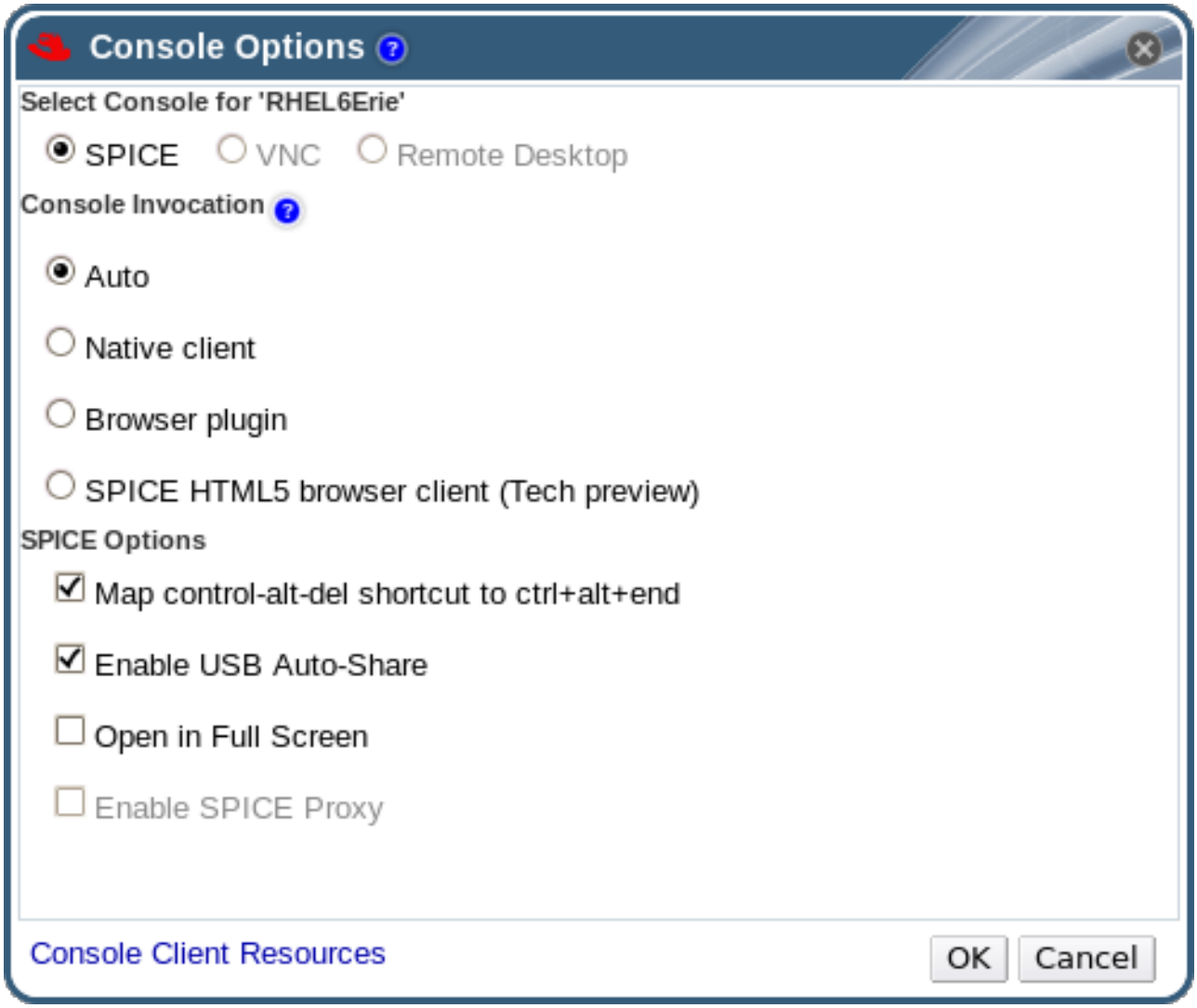


Figure 6.2. The Console Options window

Console Invocation

- **Auto**: The Manager automatically selects the method for invoking the console.
- **Native client**: When you connect to the console of the virtual machine, a file download dialog provides you with a file that opens a console to the virtual machine via Remote Viewer.
- **Browser plugin**: When you connect to the console of the virtual machine, you are connected directly via Remote Viewer.
- **SPICE HTML5 browser client (Tech preview)**: When you connect to the console of the virtual machine, a browser tab is opened that acts as the console.

SPICE Options

- **Map control-alt-del shortcut to ctrl+alt+end**: Select this check box to map the **Ctrl**+**Alt**+**Del** key combination to **Ctrl**+**Alt**+**End** inside the virtual machine.
- **Enable USB Auto-Share**: Select this check box to automatically redirect USB devices to the virtual machine. If this option is not selected, USB devices will connect to the client machine instead of the guest virtual machine. To use the USB device on the guest machine, manually enable it in the SPICE client menu.

- **Open in Full Screen**: Select this check box for the virtual machine console to automatically open in full screen when you connect to the virtual machine. Press **SHIFT**+**F11** to toggle full screen mode on or off.
- **Enable SPICE Proxy**: Select this check box to enable the SPICE proxy.
- **Enable WAN options**: Select this check box to set the parameters **WANDisableEffects** and **WANColorDepth** to **animation** and **16** bits respectively on Windows virtual machines. Bandwidth in WAN environments is limited and this option prevents certain Windows settings from consuming too much bandwidth.

Important

The **Browser plugin** console option is only available when accessing the Administration and User Portals through Internet Explorer. This console options uses the version of Remote Viewer provided by the **SpiceX.cab** installation program. For all other browsers, the **Native client** console option is the default. This console option uses the version of Remote Viewer provided by the **virt-viewer-x86.msi** and **virt-viewer-x64.msi** installation files.

6.1.4. VNC Console Options

When the VNC connection protocol is selected, the following options are available in the **Console Options** window.

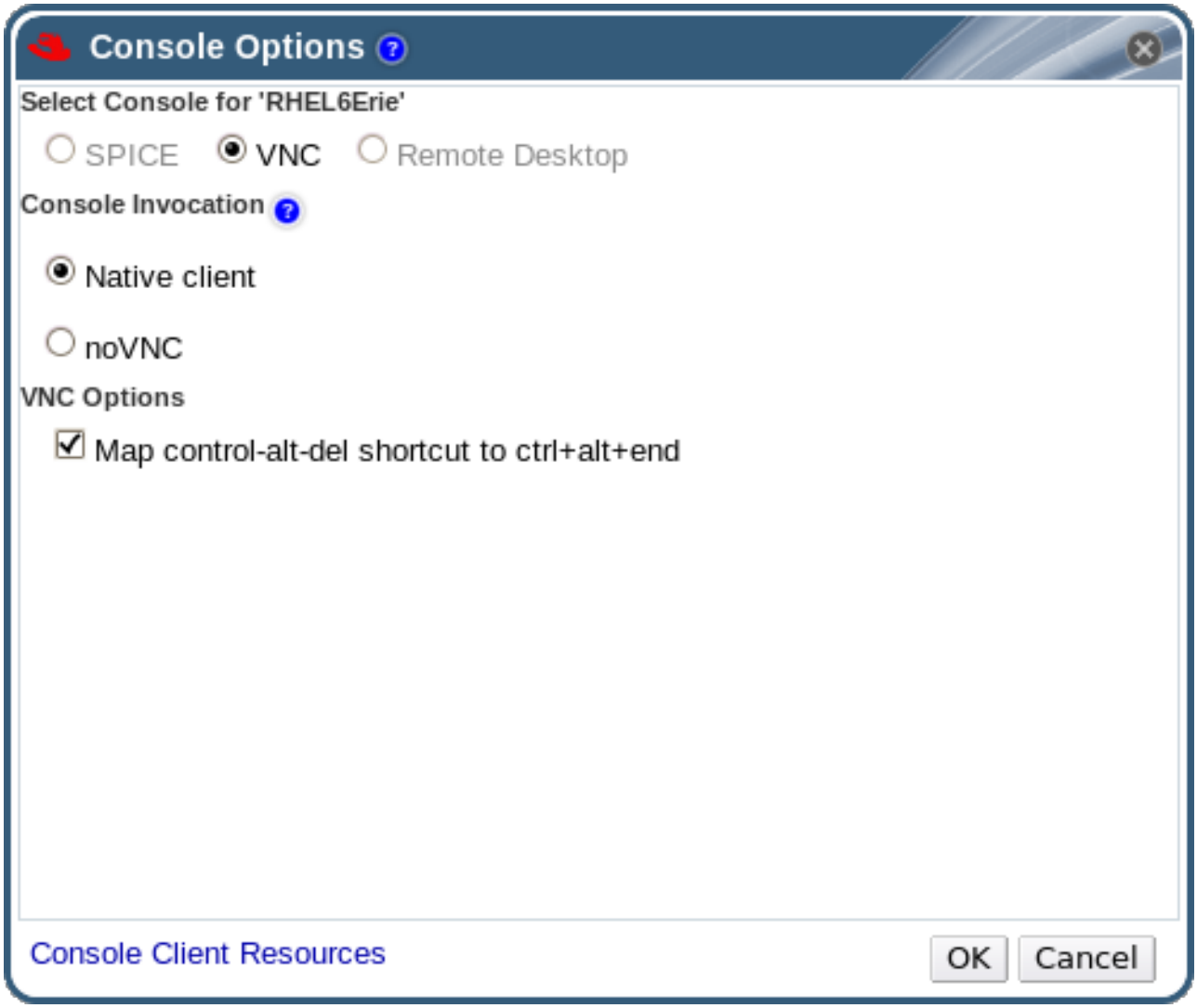


Figure 6.3. The Console Options window

Console Invocation

- **Native Client**: When you connect to the console of the virtual machine, a file download dialog provides you with a file that opens a console to the virtual machine via Remote Viewer.
- **noVNC**: When you connect to the console of the virtual machine, a browser tab is opened that acts as the console.

VNC Options

- **Map control-alt-delete shortcut to ctrl+alt+end**: Select this check box to map the **Ctrl**+**Alt**+**Del** key combination to **Ctrl**+**Alt**+**End** inside the virtual machine.

6.1.5. RDP Console Options

When the RDP connection protocol is selected, the following options are available in the **Console Options** window.

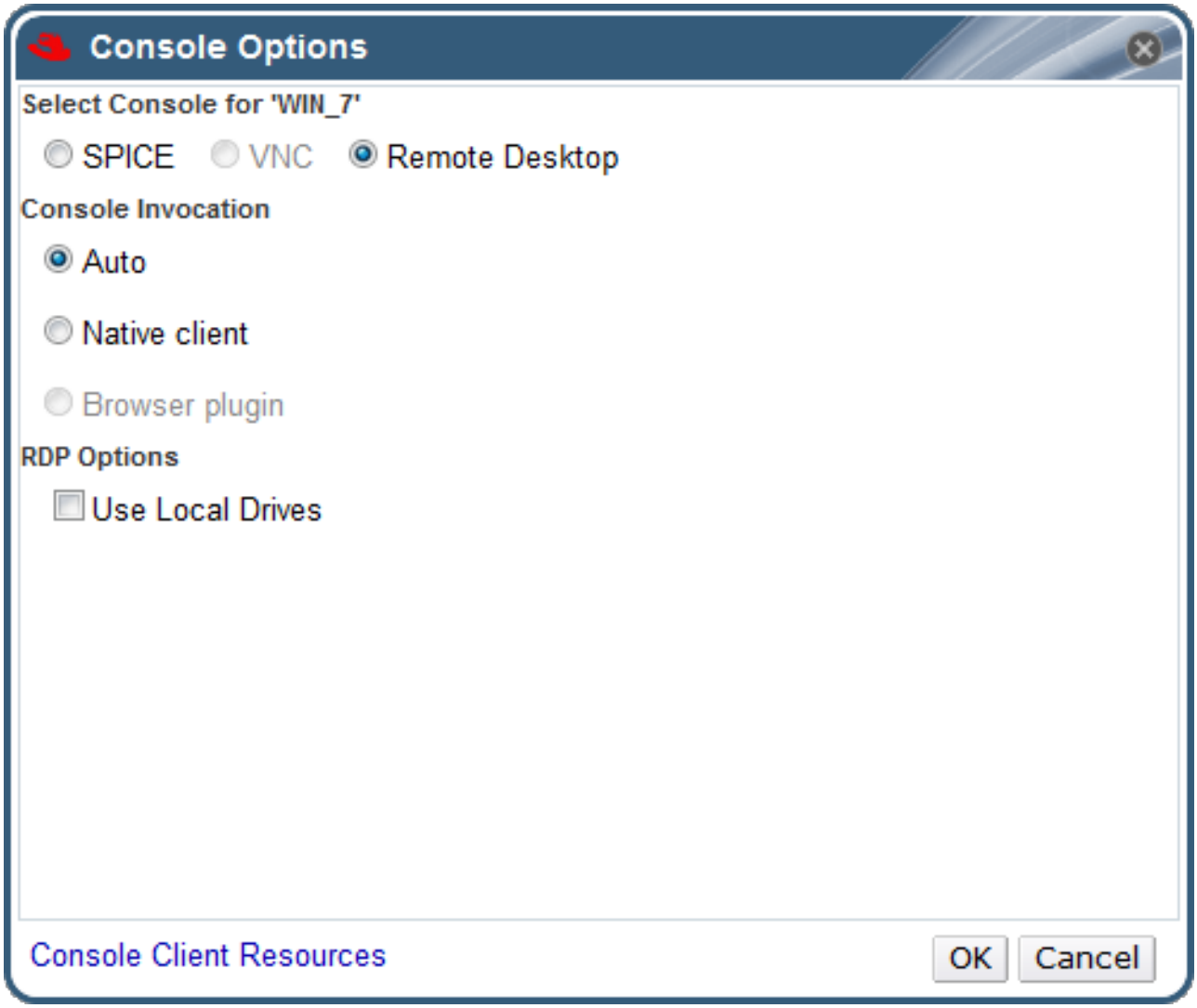


Figure 6.4. The Console Options window

Console Invocation

- **`Auto`**: The Manager automatically selects the method for invoking the console.
- **`Native client`**: When you connect to the console of the virtual machine, a file download dialog provides you with a file that opens a console to the virtual machine via Remote Desktop.

RDP Options

- **`Use Local Drives`**: Select this check box to make the drives on the client machine accessible on the guest virtual machine.

6.2. Remote Viewer Options

6.2.1. Remote Viewer Options

When you specify the **`Native client`** or **`Browser plugin`** console invocation options, you will connect to virtual machines using Remote Viewer. The Remote Viewer window provides a number of options for interacting with the virtual machine to which it is connected.

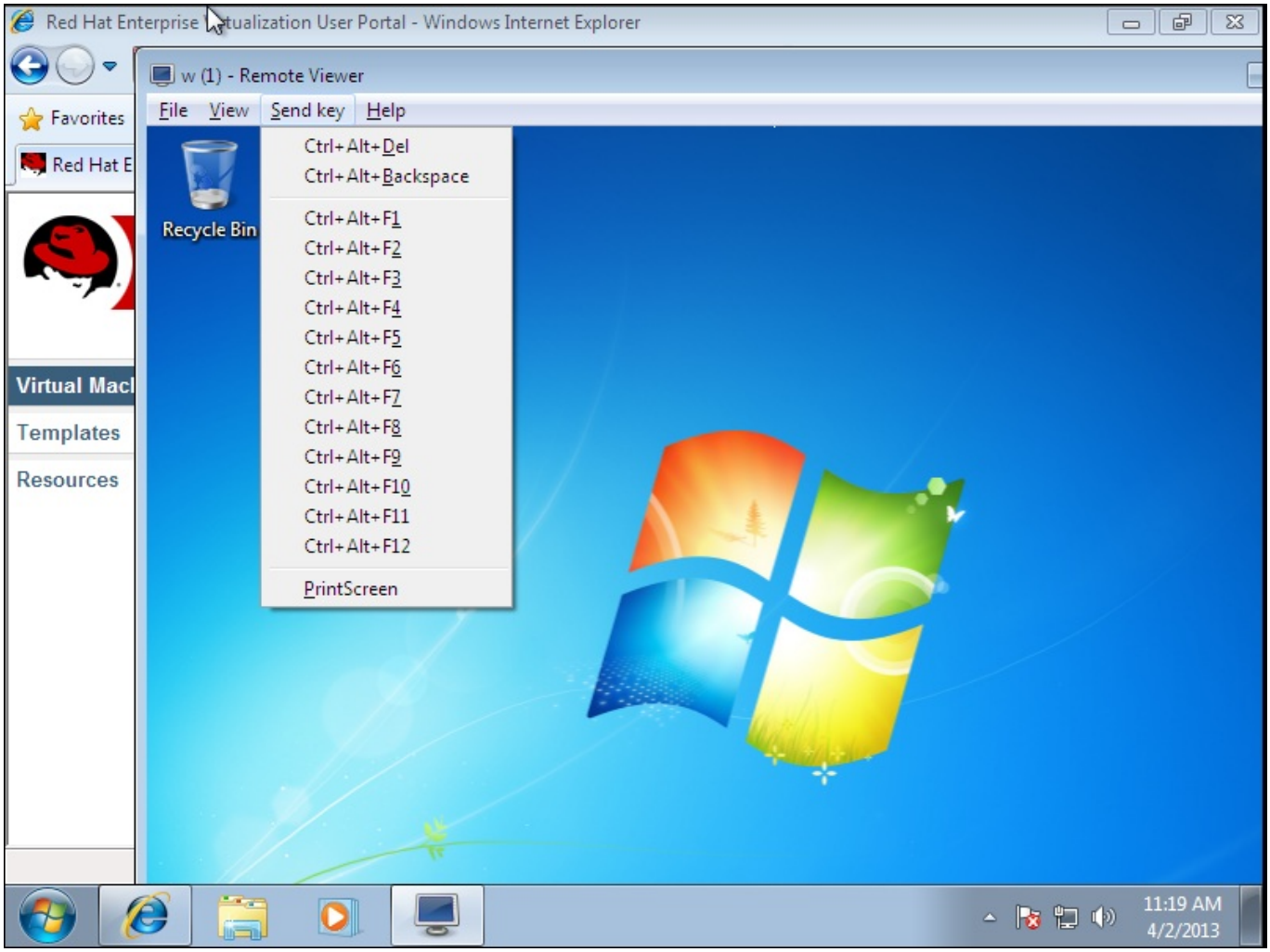


Figure 6.5. The Remote Viewer connection menu

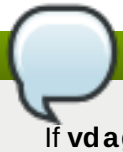
Table 6.1. Remote Viewer Options

Option	Hotkey
File	**Screenshot**: Takes a screen capture of the active window and saves it in a location of your specification. **USB device selection**: If USB redirection has been enabled on your virtual machine, the USB device plugged into your client machine can be accessed from this menu. **Quit**: Closes the console. The hot key for this option is **Shift**+**Ctrl**+**Q**.

Option	Hotkey
View	**Full screen**: Toggles full screen mode on or off. When enabled, full screen mode expands the virtual machine to fill the entire screen. When disabled, the virtual machine is displayed as a window. The hot key for enabling or disabling full screen is **SHIFT**+**F11**. **Zoom**: Zooms in and out of the console window. **Ctrl**+**+** zooms in, **Ctrl**+**-** zooms out, and **Ctrl**+**0** returns the screen to its original size. **Automatically resize**: Tick to enable the guest resolution to automatically scale according to the size of the console window. **Displays**: Allows users to enable and disable displays for the guest virtual machine.
Send key	**Ctrl**+**Alt**+**Del**: On a Red Hat Enterprise Linux virtual machine, it displays a dialog with options to suspend, shut down or restart the virtual machine. On a Windows virtual machine, it displays the task manager or Windows Security dialog. **Ctrl**+**Alt**+**Backspace**: On a Red Hat Enterprise Linux virtual machine, it restarts the X sever. On a Windows virtual machine, it does nothing. **Ctrl**+**Alt**+**F1** **Ctrl**+**Alt**+**F2** **Ctrl**+**Alt**+**F3** **Ctrl**+**Alt**+**F4** **Ctrl**+**Alt**+**F5** **Ctrl**+**Alt**+**F6** **Ctrl**+**Alt**+**F7** **Ctrl**+**Alt**+**F8** **Ctrl**+**Alt**+**F9** **Ctrl**+**Alt**+**F10** **Ctrl**+**Alt**+**F11** **Ctrl**+**Alt**+**F12** **Printscreen**: Passes the **Printscreen** keyboard option to the virtual machine.
Help	The **About** entry displays the version details of Virtual Machine Viewer that you are using.
Release Cursor from Virtual Machine	**SHIFT**+**F12**

6.2.2. Remote Viewer Hotkeys

You can access the hotkeys for a virtual machine in both full screen mode and windowed mode. If you are using full screen mode, you can display the menu containing the button for hotkeys by moving the mouse pointer to the middle of the top of the screen. If you are using windowed mode, you can access the hotkeys via the **Send key** menu on the virtual machine window title bar.



Note

If **vdagent** is not running on the client machine, the mouse can become captured in a virtual machine window if it is used inside a virtual machine and the virtual machine is not in full screen. To unlock the mouse, press **Shift**+**F12**.

Chapter 7. Configuring Multiple Monitors

7.1. Configuring Multiple Displays for Red Hat Enterprise Linux Virtual Machines

A maximum of four displays can be configured for a single Red Hat Enterprise Linux virtual machine when connecting to the virtual machine using the SPICE protocol.

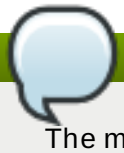
1. Start a SPICE session with the virtual machine.
2. Open the **View** drop-down menu at the top of the SPICE client window.
3. Open the **Display** menu.
4. Click the name of a display to enable or disable that display.

Note

By default, **Display 1** is the only display that is enabled on starting a SPICE session with a virtual machine. If no other displays are enabled, disabling this display will close the session.

7.2. Changing the Resolution of Displays in a Red Hat Enterprise Linux Virtual Machine

1. Open the **System** menu from the GNOME panel.
2. Open the **Preferences** section.
3. Click **Display** to open the **Display Preferences** window.
4. Select the display whose resolution is to be changed.
5. Select the resolution from the **Resolution** drop-down list.



Note

The maximum resolution that can be set for any display is 2560 x 1600. The minimum resolution that can be set for the primary display is 640 x 480; all other displays can be set to a minimum of 400 x 375.

7.3. Configuring Multiple Displays for Windows Virtual Machines

A maximum of four displays can be configured for a single Windows virtual machine when connecting to the virtual machine using the SPICE protocol.

1. Click the **Virtual Machines** tab and select a virtual machine.

2. With the virtual machine in a powered-down state, right-click the virtual machine and click **Edit** to open the **Edit Virtual Machine** window.
3. Click the **Console** tab.
4. Select the number of displays from the **Monitors** drop-down list.

Note

This setting controls the maximum number of displays that can be enabled for the virtual machine. While the virtual machine is running, additional displays can be enabled up to this number.

5. Click **Ok**.
6. Start a SPICE session with the virtual machine.
7. Open the **View** drop-down menu at the top of the SPICE client window.
8. Open the **Display** menu.
9. Click the name of a display to enable or disable that display.

Note

By default, **Display 1** is the only display that is enabled on starting a SPICE session with a virtual machine. If no other displays are enabled, disabling this display will close the session.

7.4. Changing the Resolution of Displays in a Windows Virtual Machine

The method for changing the resolution of a Windows virtual machine varies slightly in accordance with the version of Windows installed on the virtual machine. The following procedures outline how to change the resolution of virtual machines running Windows 7, Windows Vista or Windows XP.

Procedure 7.1. Windows 7

1. Right-click the desktop and click **Screen resolution** to open the **Screen Resolution** window.
2. Select the display whose resolution is to be changed.
3. Select the resolution from the **Resolution** drop-down list.

Procedure 7.2. Windows Vista

1. Right-click the desktop and click **Personalize** to open the **Personalization** section of the **Control Panel**.
2. Click **Display Settings** to open the **Display Settings** window.
3. Select the display whose resolution is to be changed.

4. Use the **Resolution** slider to change the resolution of the screen.
5. Click **Apply** to apply the new resolution.

Procedure 7.3. Windows XP

1. Right-click the desktop and click **Properties** to open the **Display Settings** window.
2. Select the display whose resolution is to be changed.
3. Use the **Resolution** slider to change the resolution of the screen.
4. Click **Apply** to apply the new resolution.

Note

The maximum resolution that can be set for any display is 2560 x 1600. The minimum resolution that can be set for the primary display is 800 x 600; all other displays can be set to a minimum of 640 x 480.

Chapter 8. Configuring USB Devices

8.1. Using USB Devices on Virtual Machines - Introduction

A virtual machine connected with the SPICE protocol can be configured to connect directly to USB devices.

The USB device will only be redirected if the virtual machine is active and in focus. USB redirection can be manually enabled each time a device is plugged in or set to automatically redirect to active virtual machines in the SPICE client menu.

Important

Note the distinction between the client machine and guest machine. The client is the hardware from which you access a guest. The guest is the virtual desktop or virtual server which is accessed through the User Portal.

8.2. Using USB Devices on Virtual Machines - Native Mode

USB redirection Native mode allows KVM/SPICE USB redirection for Linux and Windows virtual machines. Virtual (guest) machines require no guest-installed agents or drivers for native USB. All packages required by the client are brought forward by the SPICE xpi Firefox plugin. The USBClerk package must be installed on the Windows client. Native USB mode is supported on the following clients and guests:

- Client
  - Red Hat Enterprise Linux 6.0 and higher
  - Red Hat Enterprise Linux 5.5 and higher
  - Windows XP
  - Windows 7
  - Windows 2008
  - Windows 2008 Server R2
- Guest
  - Red Hat Enterprise Linux 6.0 and higher
  - Red Hat Enterprise Linux 5.5 and higher
  - Windows XP
  - Windows 7
  - Windows 2008

Note

If you have a 64-bit architecture PC, you must use the 64-bit version of Internet Explorer to install the 64-bit version of the USB driver. The USB redirection will not work if you install the 32-bit version on a 64-bit architecture. As long as you initially install the correct USB type, you then can access USB redirection from both 32 and 64-bit browsers.

8.3. Using USB Devices on a Windows Client

The **usbclerk** service must be running on the Windows client for the USB device to be redirected to the guest. Ensure the version of **usbclerk** matches the architecture of the client machine. For example, the 64-bit version of **usbclerk** must be installed on 64-bit Windows machines.

Procedure 8.1. Using USB Devices on a Windows Client

1. When the **usbclerk** service is installed and running, select a virtual machine that has been configured to use the SPICE protocol.
2. Ensure USB support is set to **Native**:
    a. Click the **Edit** button to open the **Edit Virtual Machine** window.
    b. Click the **Console** tab.
    c. From the **USB Support** drop-down menu, select **Native**.
    d. Click **OK**.
3. Right-click the virtual machine and click **Edit Console Options** to open the **Console Options** window, and select the **Enable USB Auto-Share** check box.
4. Start the virtual machine and click the **Console** button to connect to that virtual machine. When you plug your USB device into the client machine, it will automatically be redirected to appear on your guest machine.

8.4. Using USB Devices on a Red Hat Enterprise Linux Client

The *usbredir* package enables USB redirection from Red Hat Enterprise Linux clients to virtual machines. *usbredir* is a dependency of the *spice-xpi* package, and is automatically installed together with that package.

Procedure 8.2. Using USB devices on a Red Hat Enterprise Linux client

1. Click the **Virtual Machines** tab and select a virtual machine that has been configured to use the SPICE protocol.
2. Ensure USB support is set to **Native**:
    a. Click the **Edit** button to open the **Edit Virtual Machine window.**
    b. Click the **Console** tab.
    c. From the **USB Support** drop-down menu, select **Native**.
    d. Click **OK**.

3. Right-click the virtual machine and click **Edit Console Options** to open the **Console Options** window, and select the **Enable USB Auto-Share** check box.

4. Start the virtual machine and click the **Console** button to connect to that virtual machine. When you plug your USB device into the client machine, it will automatically be redirected to appear on your guest machine.

8.5. Using USB Devices on Virtual Machines - Legacy Mode

Legacy mode for USB redirection enables the SPICE USB redirection policy used in Red Hat Enterprise Virtualization 3.0. Legacy mode must be manually configured.

Legacy USB mode is supported on the following clients and guests:

- Client
  - Red Hat Enterprise Linux 6.0 and higher
  - Red Hat Enterprise Linux 5.5 and higher
  - Windows XP
  - Windows 7
  - Windows 2008
- Guest
  - Windows XP
  - Windows 7

Configuring a Linux Client to Use USB Redirection in Legacy Mode

If you connect to a virtual guest from a Red Hat Enterprise Linux client machine, you have to install several SPICE packages before you can share USB devices between the client and the guest.

Procedure 8.3. Using USB devices on Red Hat Enterprise Linux clients:

1. **Install SPICE packages on client**

   On your Linux client machine, install the following packages:

   - *spice-usb-share*
   - *kmod-kspiceusb-rhel60* for Red Hat Enterprise Linux 6 or

     kmod-kspiceusb-rhel5u6 for Red Hat Enterprise Linux 5

   These packages are available on the Content Delivery Network, from the Red Hat Enterprise Linux Supplementary Software channel for your version of Red Hat Enterprise Linux. To install the packages, run:

   ```
   # yum install spice-usb-share kmod-kspiceusb
   ```

2. **Run SPICE USB services**

   Start the **spiceusbsrvd** service and load the **kspiceusb** module. Run:

```
# service spiceusbsrvd start
# modprobe kspiceusb
```

3. **Install RHEV-Tools on guest**

   Locate the CD drive to access the contents of the Guest Tools ISO, and launch **RHEV-ToolsSetup.exe**. If the Guest Tools ISO is not available in your CD drive, contact your system administrator. After the tools have been installed, you will be prompted to restart the machine for changes to be applied.

4. **Open firewall ports**

   Allow connections on TCP port 32023 on any firewalls between the guest machine and the client machine.

5. **Enable USB Auto-Share**

   On the User Portal, select your guest machine. Ensure that you have enabled SPICE USB Auto-Share on the guest machine.

6. **Attach USB device**

   Connect to your guest machine. Place the SPICE console window of your guest desktop in focus, then attach a USB device to the client. The USB device displays in your guest desktop.

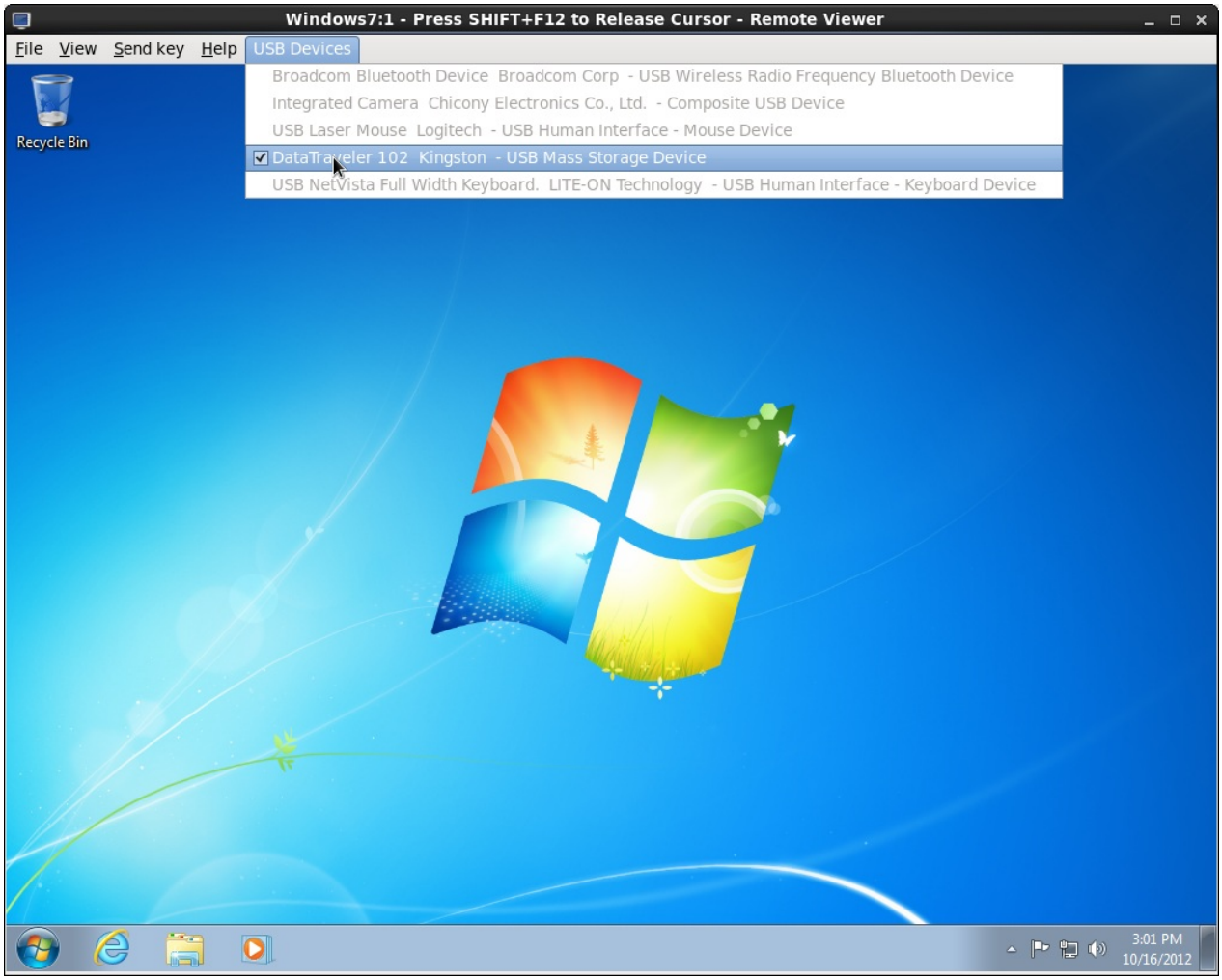
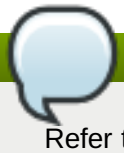

Windows7:1 - Press SHIFT+F12 to Release Cursor - Remote Viewer
File View Send key Help USB Devices
Broadcom Bluetooth Device Broadcom Corp - USB Wireless Radio Frequency Bluetooth Device
Integrated Camera Chicony Electronics Co., Ltd. - Composite USB Device
USB Laser Mouse Logitech - USB Human Interface - Mouse Device
DataTraveler 102 Kingston - USB Mass Storage Device
USB NetVista Full Width Keyboard. LITE-ON Technology - USB Human Interface - Keyboard Device
Recycle Bin
3:01 PM
10/16/2012

Figure 8.1. List of Connected USB devices - Linux Client

When you close the SPICE session the USB device will no longer be shared with the guest.

Configuring a Windows Client to Use USB Redirection in Legacy Mode

If you are connecting from a Windows client machine, and wish to use USB devices on your guest, you have to enable SPICE USB redirection.



Note

Refer to the *Red Hat Enterprise Virtualization Manager Release Notes* for specific channel names current to your system.

Procedure 8.4. Enabling USB redirection on Windows:

1. **Install USB redirector package on client**

   On a Windows client machine, install **RHEV-USB-Client.exe**. This package can be obtained from the **Red Hat Enterprise Virtualization Manager (v.3.5 x86_64)** channel on the Content Delivery Network, under the **Downloads** list.

2. **Install RHEV-Tools on guest**

   Locate the CD drive to access the contents of the Guest Tools ISO, and launch **RHEV-ToolsSetup.exe**. If the Guest Tools ISO is not available in your CD drive, contact your system administrator. After the tools have been installed, you will be prompted to restart the machine for changes to be applied.

3. **Open firewall ports**

   Allow connections on TCP port 32023 on any firewalls between the guest machine and the client machine.

4. **Enable USB sharing**

   On the User Portal, select your guest machine. Ensure that you have enabled SPICE USB sharing on the guest machine.

5. **Attach USB device**

   Connect to your guest machine and attach a USB device to the client. If the required USB device does not appear directly on the guest desktop, right-click on the SPICE frame and select **USB Devices**. Choose your device from the list displayed.

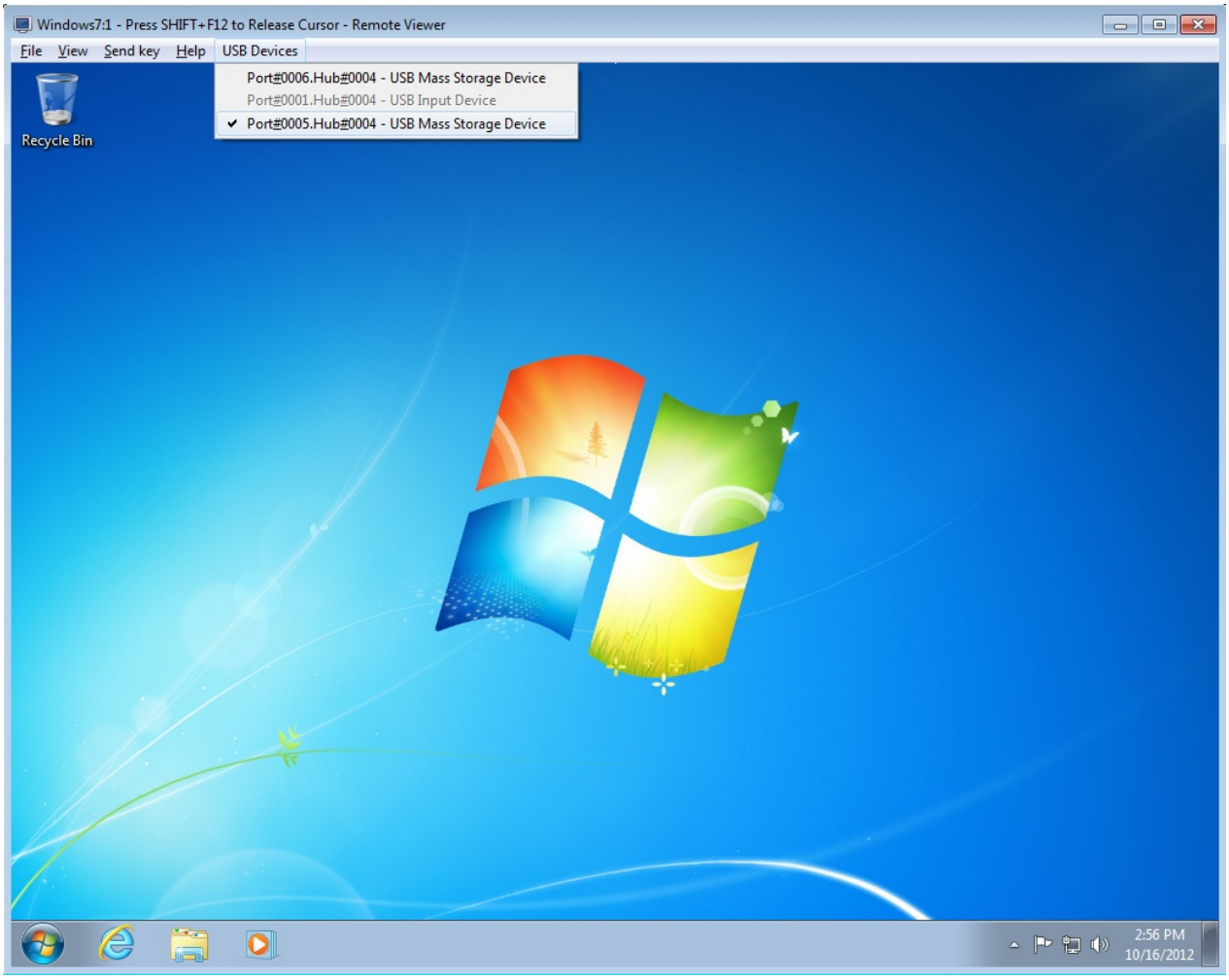

Windows7:1 - Press SHIFT+F12 to Release Cursor - Remote Viewer
File View Send key Help USB Devices
Port#0006.Hub#0004 - USB Mass Storage Device
Port#0001.Hub#0004 - USB Input Device
Port#0005.Hub#0004 - USB Mass Storage Device
Recycle Bin
2:56 PM
10/16/2012

Figure 8.2. List of connected USB devices

Important

When some USB devices are connected on Windows clients, the autoplay window will appear and the client will take control of the device, making it unavailable to the guest. To avoid this issue, disable USB autoplay on your Windows clients.

Note

You can also define additional USB policies for Windows clients, to allow or block access to certain USB devices. For details, see the sections on USB Filter Editor in the *Red Hat Enterprise Virtualization Administration Guide*.

8.6. Configuring a Linux Client to Use USB Redirection in Legacy Mode

If you connect to a virtual guest from a Red Hat Enterprise Linux client machine, you have to install several SPICE packages before you can share USB devices between the client and the guest.

Procedure 8.5. Using USB devices on Red Hat Enterprise Linux clients:

1. **Install SPICE packages on client**

   On your Linux client machine, install the following packages:

   - *spice-usb-share*
   - *kmod-kspiceusb-rhel60* for Red Hat Enterprise Linux 6 or

     kmod-kspiceusb-rhel5u6 for Red Hat Enterprise Linux 5

   These packages are available on the Content Delivery Network, from the Red Hat Enterprise Linux Supplementary Software channel for your version of Red Hat Enterprise Linux. To install the packages, run:

   ```
   # yum install spice-usb-share kmod-kspiceusb
   ```

2. **Run SPICE USB services**

   Start the **spiceusbsrvd** service and load the **kspiceusb** module. Run:

   ```
   # service spiceusbsrvd start
   # modprobe kspiceusb
   ```

3. **Install RHEV-Tools on guest**

   Locate the CD drive to access the contents of the Guest Tools ISO, and launch **RHEV-ToolsSetup.exe**. If the Guest Tools ISO is not available in your CD drive, contact your system administrator. After the tools have been installed, you will be prompted to restart the machine for changes to be applied.

4. **Open firewall ports**

   Allow connections on TCP port 32023 on any firewalls between the guest machine and the client machine.

5. **Enable USB Auto-Share**

   On the User Portal, select your guest machine. Ensure that you have enabled SPICE USB Auto-Share on the guest machine.

6. **Attach USB device**

   Connect to your guest machine. Place the SPICE console window of your guest desktop in focus, then attach a USB device to the client. The USB device displays in your guest desktop.

When you close the SPICE session the USB device will no longer be shared with the guest.

8.7. Configuring a Windows Client to Use USB Redirection in Legacy Mode

If you are connecting from a Windows client machine, and wish to use USB devices on your guest, you have to enable SPICE USB redirection.

Note

See the *Red Hat Enterprise Virtualization Manager Release Notes* for specific channel names current to your system.

Procedure 8.6. To enable USB redirection on Windows:

1. **Install USB redirector package on client**

   On a Windows client machine, install the **RHEV-USB-Client.exe**. This package can be obtained from the **Red Hat Enterprise Virtualization Manager (v.3.5 x86_64)** channel on the Content Delivery Network, under the **Downloads** list.

2. **Install RHEV-Tools on guest**

   Locate the CD drive to access the contents of the Guest Tools ISO, and launch **RHEV-ToolsSetup.exe**. If the Guest Tools ISO is not available in your CD drive, contact your system administrator. After the tools have been installed, you will be prompted to restart the machine for changes to be applied.

3. **Open firewall ports**

   Allow connections on TCP port 32023 on any firewalls between the guest machine and the client machine.

4. **Enable USB sharing**

   On the User Portal, select your guest machine. Ensure that you have enabled SPICE USB sharing on the guest machine.

5. **Attach USB device**

   Connect to your guest machine and attach a USB device to the client. If the required USB device does not appear directly on the guest desktop, right-click on the SPICE frame and select **USB Devices**. Choose your device from the list displayed.

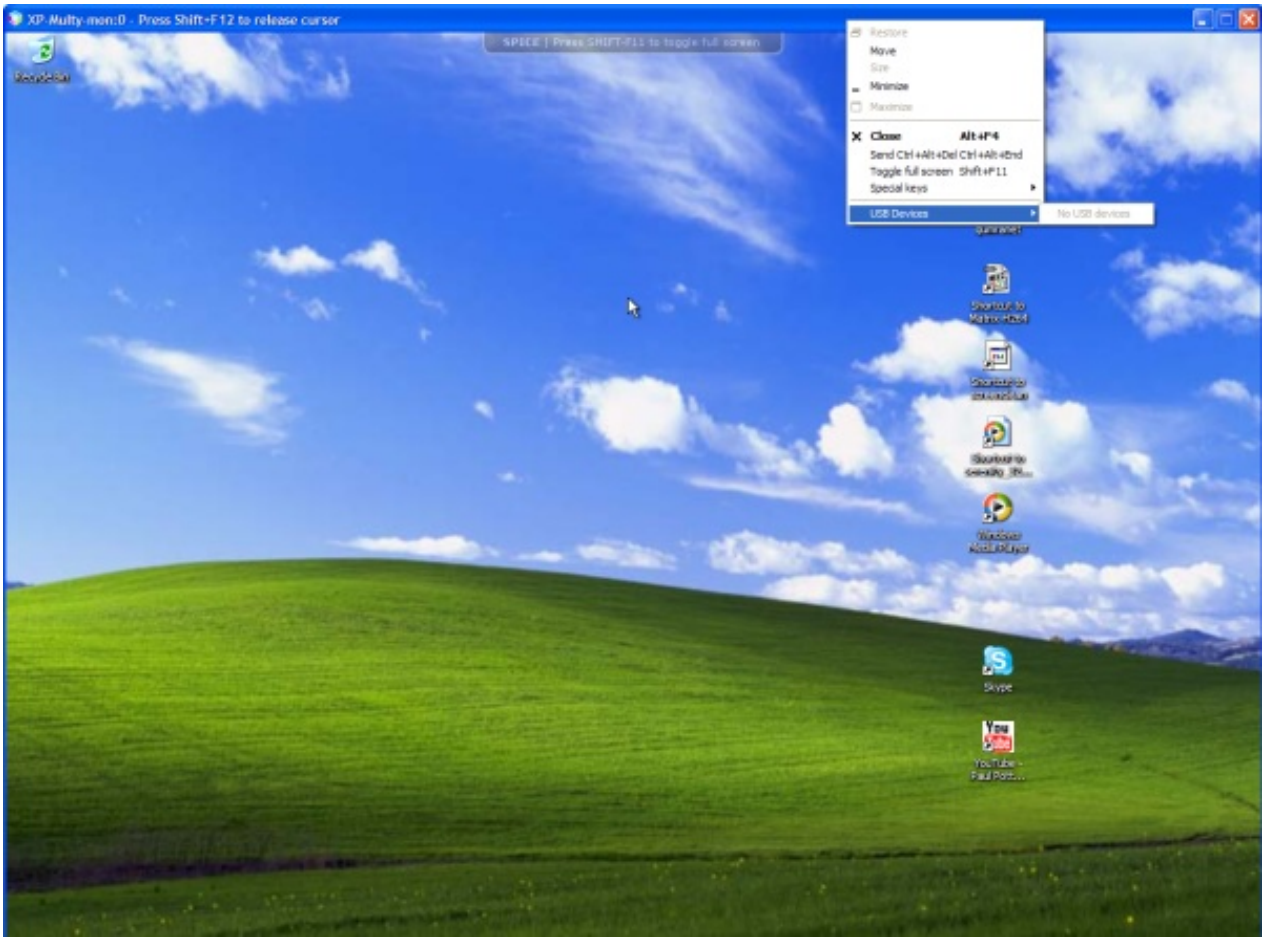


Figure 8.3. List of connected USB devices

Important

When some USB devices are connected on Windows clients, the autoplay window will appear and the client will take control of the device, making it unavailable to the guest. To avoid this issue, disable USB autoplay on your Windows clients.

Note

You can also define additional USB policies for Windows clients, to allow or block access to certain USB devices. For details, see the sections on USB Filter Editor in the *Red Hat Enterprise Virtualization Administration Guide*.

Chapter 9. Configuring Single Sign-On for Virtual Machines

9.1. Configuring Single Sign-On for Virtual Machines

Configuring single sign-on, also known as password delegation, allows you to automatically log in to a virtual machine using the credentials you use to log in to the User Portal. Single sign-on can be used on both Red Hat Enterprise Linux and Windows virtual machines.

Important

If single sign-on to the User Portal is enabled, single sign-on to virtual machines will not be possible. With single sign-on to the User Portal enabled, the User Portal does not need to accept a password, thus the password cannot be delegated to sign in to virtual machines.

9.2. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines Using IPA (IdM)

To configure single sign-on for Red Hat Enterprise Linux virtual machines using GNOME and KDE graphical desktop environments and IPA (IdM) servers, you must install the *rhevm-guest-agent* package on the virtual machine and install the packages associated with your window manager.

Important

The following procedure assumes that you have a working IPA configuration and that the IPA domain is already joined to the Manager. You must also ensure that the clocks on the Manager, the virtual machine and the system on which IPA (IdM) is hosted are synchronized using NTP.

Procedure 9.1. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines

1. Log in to the Red Hat Enterprise Linux virtual machine.
2. Enable the required channel:
   - For Red Hat Enterprise Linux 6

     ```
     # subscription-manager repos --enable=rhel-6-server-rhev-agent-rpms
     ```

   - For Red Hat Enterprise Linux 7

     ```
     # subscription-manager repos --enable=rhel-7-server-rh-common-rpms
     ```

3. Run the following command to download and install the guest agent packages:

   ```
   # yum install rhevm-guest-agent-common
   ```

4. Run the following commands to install the single sign-on packages:

```
# yum install rhev-agent-pam-rhev-cred
# yum install rhev-agent-gdm-plugin-rhevcred
```

5. Run the following command to install the IPA packages:

```
# yum install ipa-client
```

6. Run the following command and follow the prompts to configure **ipa-client** and join the virtual machine to the domain:

```
# ipa-client-install --permit --mkhomedir
```

Note

In environments that use DNS obfuscation, this command should be:

```
# ipa-client-install --domain=[FQDN] --server==[FQDN]
```

7. Fetch the details of an IPA user:

```
# getent passwd [IPA user name]
```

This will return something like this:

```
[some-ipa-user]:*:936600010:936600001::/home/[some-ipa-user]:/bin/sh
```

You will need this information in the next step to create a home directory for *[some-ipa-user]*.

8. Set up a home directory for the IPA user:

    a. Create the new user's home directory:

    ```
    # mkdir /home/[some-ipa-user]
    ```

    b. Give the new user ownership of the new user's home directory:

    ```
    # chown 935500010:936600001 /home/[some-ipa-user]
    ```

Result

You have enabled single sign-on for your Red Hat Enterprise Linux virtual machine. Log in to the User Portal using the user name and password of a user configured to use single sign-on and connect to the console of the virtual machine. You will be logged in automatically.

9.3. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines Using Active Directory

To configure single sign-on for Red Hat Enterprise Linux virtual machines using GNOME and KDE graphical desktop environments and Active Directory, you must install the *rhevm-guest-agent* package on the virtual machine, install the packages associated with your window manager and join the virtual machine to the domain.

Important

The following procedure assumes that you have a working Active Directory configuration and that the Active Directory domain is already joined to the Manager. You must also ensure that the clocks on the Manager, the virtual machine and the system on which Active Directory is hosted are synchronized using NTP.

Procedure 9.2. Configuring Single Sign-On for Red Hat Enterprise Linux Virtual Machines

1. Log in to the Red Hat Enterprise Linux virtual machine.
2. Enable the Red Hat Enterprise Virtualization Agent channel:
   - For Red Hat Enterprise Linux 6

     ```
     # subscription-manager repos --enable=rhel-6-server-rhev-agent-rpms
     ```

   - For Red Hat Enterprise Linux 7

     ```
     # subscription-manager repos --enable=rhel-7-server-rh-common-rpms
     ```

3. Run the following command to download and install the guest agent packages:

   ```
   # yum install rhevm-guest-agent-common
   ```

4. Run the following command to install the single sign-on packages:

   ```
   # yum install rhev-agent-gdm-plugin-rhevcred
   ```

5. Run the following command to install the Samba client packages:

   ```
   # yum install samba-client samba-winbind samba-winbind-clients
   ```

6. On the virtual machine, modify the **/etc/samba/smb.conf** file to contain the following, replacing **DOMAIN** with the short domain name and **REALM.LOCAL** with the Active Directory realm:

   ```
   [global]
      workgroup = DOMAIN
      realm = REALM.LOCAL
      log level = 2
      syslog = 0
      server string = Linux File Server
   ```

```
    security = ads
    log file = /var/log/samba/%m
    max log size = 50
    printcap name = cups
    printing = cups
    winbind enum users = Yes
    winbind enum groups = Yes
    winbind use default domain = true
    winbind separator = +
    idmap uid = 1000000-2000000
    idmap gid = 1000000-2000000
    template shell = /bin/bash
```

7. Run the following command to join the virtual machine to the domain:

```
net ads join -U [user name]
```

8. Run the following command to start the **winbind** service and ensure it starts on boot:

```
# service winbind start
# chkconfig winbind on
```

9. Run the following commands to verify that the system can communicate with Active Directory:
   - Verify that a trust relationship has been created:

```
# wbinfo -t
```

   - Verify that you can list users:

```
# wbinfo -u
```

   - Verify that you can list groups:

```
# wbinfo -g
```

10. Run the following command to configure the NSS and PAM stack:
    a. Run the following command to open the **Authentication Configuration** window:

```
# authconfig-tui
```

    b. Select the **Use Winbind** check box, select **Next** and press **Enter**.
    c. Select the **OK** button and press **Enter**.

Result

You have enabled single sign-on for your Red Hat Enterprise Linux virtual machine. Log in to the User Portal using the user name and password of a user configured to use single sign-on and connect to the console of the virtual machine. You will be logged in automatically.

9.4. Configuring Single Sign-On for Windows Virtual Machines

To configure single sign-on for Windows virtual machines, the Windows guest agent must be installed on the guest virtual machine. The **RHEV Guest Tools** ISO file provides this agent. If the **RHEV-toolsSetup.iso** image is not available in your ISO domain, contact your system administrator.

Procedure 9.3. Configuring Single Sign-On for Windows Virtual Machines

1. From the **Extended** tab of the User Portal, select the Windows virtual machine. Ensure the machine is powered up, then click the **Change CD** button.
2. From the list of images, select **RHEV-toolsSetup.iso**. Click **OK**.
3. Once you have attached the guest tools, click the **Console** icon and log in to the virtual machine.
4. On the virtual machine, locate the CD drive to access the contents of the guest tools ISO file and launch **RHEV-ToolsSetup.exe**. After the tools have been installed, you will be prompted to restart the machine to apply the changes.

Result

You have enabled single sign-on for your Windows virtual machine. Log in to the User Portal using the user name and password of a user configured to use single sign-on and connect to the console of the virtual machine. You will be logged in automatically.

9.5. Disabling Single Sign-on for Virtual Machines

The following procedure explains how to disable single sign-on for a virtual machine.

Procedure 9.4. Disabling SSO for virtual machines

1. From the User Portal **Extended** tab, select a virtual machine and click **Edit**.
2. Select the **Console** tab and select the check box labeled **Disable Single Sign On**, and then click **OK**.

Revision History

Revision 3.5-24	**Wed 11 Mar 2015**	**Red Hat Enterprise Virtualization Documentation Team**

BZ#1180932 - Removed a topic on configuring single sign-on to the User Portal and Administration Portal, because this is an administrative user task.

Revision 3.5-23	**Mon 09 Feb 2015**	**Julie Wu**

BZ#1075477 - Created a new topic on disabling SSO for virtual machines and other minor edits.

Revision 3.5-22	**Mon 19 Jan 2015**	**David Ryan**

BZ#1153351 - Updated the supported management client configurations.

Revision 3.5-21	**Thur 11 Dec 2014**	**Julie Wu**

BZ#1121762 - Created a topic on single sign-on to the Administration or User Portal.

Revision 3.5-20	**Tues 25 Nov 2014**	**Tahlia Richardson**

BZ#1120921 - Updated the Initial Run row of the Run Once settings table.

Revision 3.5-19	**Tues 18 Nov 2014**	**Lucy Bopf**

BZ#1157459 - Corrected the procedure for setting a Windows product key.

Revision 3.5-18	**Mon 20 Oct 2014**	**Laura Novich**

Minor line edits to improve consistency.

Revision 3.5-17	**Fri 17 Oct 2014**	**Tahlia Richardson**

BZ#1120916 - Expanded the Random Generator Settings Explained table with additional options.

Revision 3.5-16	**Mon 13 Oct 2014**	**Julie Wu**

BZ#1139846 - Updated RHEV guest agent channel for RHEL 7.

Revision 3.5-15	**Sun 12 Oct 2014**	**Laura Novich**

BZ#1120923 - Changed directions for ejecting and changing a CD".

Revision 3.5-14	**Fri 19 Sep 2014**	**Tahlia Richardson**

BZ#1143841 - Removed references to RHN Classic and replaced "Red Hat Network" with "Content Delivery Network".

Revision 3.5-13	**Thu 18 Sep 2014**	**Lucy Bopf**

BZ#1143777 - Updated screen shots for the User Portal.

Revision 3.5-12	**Thu 18 Sep 2014**	**Andrew Burden**

Brewing for 3.5-Beta.

Revision 3.5-11	**Thu 11 Sep 2014**	**Laura Novich**

BZ#1120923 - Instructions changed for changing the CD window.

Revision 3.5-10	**Wed 10 Sep 2014**	**Julie Wu**

Building for splash page.

Revision 3.5-9 **Fri 29 Aug 2014** **Tahlia Richardson**

BZ#1134151 - Added a row about instance types to the New/Edit VM explanation tables.

Revision 3.5-8 **Mon 25 Aug 2014** **Tahlia Richardson**

BZ#1120944 - Amended virtual machine name maximum character limit to 255.
BZ#1120916 - Added a new topic detailing the Random Generator tab, and added Random Generator to lists of tabs in other topics.
BZ#1120918 - Added new rows to the table in Virtual Machine System Settings Explained, detailing the new 'custom serial number' option.

Revision 3.5-7 **Wed 20 Aug 2014** **Andrew Dahms**

BZ#1131761 - Updated the list of options available in the Initial Run tab for virtual machines.
BZ#1131718 - Added a note about storage space requirements when deleting virtual machine snapshots.
BZ#1122304 - Added a note on new command line options for installing the guest agents and drive on Windows.

Revision 3.5-6 **Mon 18 Aug 2014** **Tahlia Richardson**

BZ#1120955 - Updated the section on 'editing a virtual machine' to reflect new behaviour.
BZ#1124078 - Added a procedure for the new Clone VM button in the User Portal.

Revision 3.5-5 **Fri 8 Aug 2014** **Andrew Dahms**

BZ#1127943 - Updated the procedure for deleting virtual machine snapshots.
BZ#1042817 - Updated the description of RDP console options.

Revision 3.5-4 **Wed 23 Jul 2014** **Lucy Bopf**

BZ#1122072 - Updated the Enable WAN Options description to include more detail.

Revision 3.5-3 **Fri 27 Jun 2014** **Andrew Dahms**

BZ#1093492 - Outlined the difference between the methods for sealing a Linux virtual machine.
BZ#1068759 - Added information on the name of services and location of configuration files for the guest agents.
BZ#1012841 - Added separate procedures on how to import the Manager certificate.

Revision 3.5-2 **Fri 6 Jun 2014** **Andrew Dahms**

BZ#996570 - Updated the list of console options for the SPICE and VNC connection protocols.

Revision 3.5-1 **Thu 5 Jun 2014** **Lucy Bopf**

Initial creation for the Red Hat Enterprise Virtualization 3.5 release.